LOW COST, LOW COMPLEXITY SENSOR DESIGN FOR NON-COOPERATIVE GEOLOCATION VIA RECEIVED SIGNAL STRENGTH

THESIS

Michael S. Butler, Captain, USAF

AFIT/GE/ENG/12-05

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT/GE/ENG/12-05

LOW COST, LOW COMPLEXITY SENSOR DESIGN FOR NON-COOPERATIVE GEOLOCATION VIA RECEIVED SIGNAL STRENGTH

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Electrical Engineering

Michael S. Butler, B.S.E.E.

Captain, USAF

March 2012

AFIT/GE/ENG/12-05

LOW COST, LOW COMPLEXITY SENSOR DESIGN FOR NON-COOPERATIVE GEOLOCATION VIA RECEIVED SIGNAL STRENGTH

Michael S. Butler, B.S.E.E.

Captain, USAF

Approved:

/signed/	1 Mar 2012
Dr. Richard K. Martin (Chairman)	date
/signed/	1 Mar 2012
Maj. Mark D. Silvius, PhD (Member)	date
/signed/	1 Mar 2012
Maj. Todd R. Andel, PhD (Member)	date

AFIT/GE/ENG/12-05

Abstract

Obtaining accurate non-cooperative geolocation is vital for persistent surveillance of a hostile emitter. Current research for developing a small, low cost, low complexity and energy efficient sensor network for non-cooperative geolocation measurements via received signal strength (RSS) is limited. Most existing work focuses on simulating a non-cooperative network (NN) and in doing so, simulated models often ignore localization errors caused from the hardware processing raw RSS data and often model environment-dependent errors as random. By comparing real-time measured non-cooperative geolocation data to a simulated system, a more accurate model can be developed.

The main focus of this research effort is designing a Poor Man's Spectrum Analyzer (PMSA) to locate a wireless device in a non-cooperative network (NN) that is transmitting in the Industrial, Scientific and Medical (ISM) radio band of 2.403 GHz to 2.48 GHz by measuring the emitter's received signal strength (RSS). The PMSA will analyze electrical signals that are passing through or being transmitted by a system or device. By interfacing a PMSA with an embedded controller that could take the form of a wireless sensor, visual detection and analysis of electromagnetic signals over the ISM band of frequencies can be made. Geolocation is performed from the PMSA's ability in measuring the RSS of a NN.

The modeling of the sensor motes are based on the PMSA/SPOT prototype device. Two sensor network configurations are deployed to the field to determine the operational capability in geolocating one non-cooperative network at a time placed in three locations. Operational capability is evaluated by comparing the measured and simulated results to the Cramer-Rao Lower Bound (CRLB) and covariance error ellipses. This thesis discusses the development and performance of a small, low cost, low complexity, and energy efficient sensor network that can locate a NN via RSS.

Acknowledgements

First and foremost I would like to thank my thesis advisor, Dr. Richard Martin. Without his guidance and support throughout this research effort I would not have been able to complete it. His technical expertise, advice, and patience he shared with me were greatly appreciated.

I would like to thank all of my friends in the RSFEL lab. Their company and interesting debate topics made the long frustrating days bearable. I would like to extend my sincere appreciation to Charles McNeeley and Russell Lenehan for sharing their technical expertise with me regarding circuit components and Java programming.

Finally, I would like to thank my incredible wife, for her love and support. I will have spent 18 out of the first 22 months of our marriage putting my heart and soul into AFIT instead of our marriage. I am sorry honey that I did not find a happy balance.

Michael S. Butler

Table of Contents

Page

List of Figures

List of Tables

List of Abbreviations

Abbreviation		Page
AWGN	Additive White Gaussian Noise	15
RMSE	Root MSE	18
QC	Quality Control	23
LRIP	Low Rate Initial Production	23
FRPDR	Full Rate Production Decision Review	23
C2	Command and Control	23
BP	Bandpass	26
VCO	Voltage Controlled Oscillator	26
Op-amps	Operational Amplifiers	27
IF	Intermediate Frequency	27
VR	Variable Resistor	27
CLK	Clock Pin	27
CS	Chip Select	27
U/D	Up/Down	27
ADC	Analog-to-Digital Converter	29
LS	Least Squares	42
PDF	Probability Density Function	52
FRP	Full Rate Production	53
FOC	Full Operational Capability	53
WARP	Wireless Open Access Research Platform	56
NaN	Not a Number	60

LOW COST, LOW COMPLEXITY SENSOR DESIGN FOR NON-COOPERATIVE GEOLOCATION VIA RECEIVED SIGNAL STRENGTH

I. Introduction

This chapter describes relevant background material for this research effort, including applications, types of wireless networks, and the hardware devices that were used. The motivation and research objectives for this effort are also be discussed.

1.1 Background

The problem of locating and tracking signal-emitting sources has attracted attention for the last 60 years. Early applications in radar and sonar typically involved a few sensors. In the last six decades, there has been a considerable increase in the sophistication of wireless networks [14]. Dramatic advances in *Radio Frequency* (RF) have been made possible through the use of large networks of wireless sensors for a variety of new monitoring and control applications. These advancements have led to the broadening of techniques employed for localization as well as the applications where localization is important. Examples of today's applications that serve as the major driving force for current research efforts include [27]:

- Monitoring and tracking for security reasons
- Location based billing
- Fraud protection
- Asset tracking
- Fleet management
- Alternative to *Global Positioning System* (GPS) navigation

Due to the increased quantity of wireless devices and their applications used today, *Wireless Network Discovery* (WND) is employed to discover and analyze important properties and characteristics of these devices. The properties and characteristics include, but are not limited to [16]:

- The transmitting frequency of the device
- The real-world geographic location of the device
- Communication patterns
- Type of information being shared
- Antenna patterns on the device
- Signal strength
- Effects of the surrounding environment on transmitted signal

A wireless network user can utilize WND to discover information about two types of network devices. The first is a *cooperative network* (CN). A CN has the capability to share information in a peer-to-peer manner such as positioning measurements between the primary user and emitter [25]. The primary user in this thesis is defined as the sensor network. If the locations of the emitter are unknown, the primary user might have *a priori* knowledge of the last positioning coordinates to formulate localization estimates. This is often the case when a device in a CN is not complex enough to know its own location or other important statistics, as seen with large, inexpensive sensor networks [16]. An example of a CN is the geolocation of emergency 911 calls from mobile phone users by using the transmitting signals from cell towers.

The second type of network is a *non-cooperative network* (NN). A NN in this thesis is defined as a device or network of devices operated by an outside user. WND on a NN is not directly available to the sensor network [16]. An example of WND non-availability might be an attack on a sensor network from a hostile emitter. The sensor network may not have *a priori* knowledge of the hostile emitter's location because

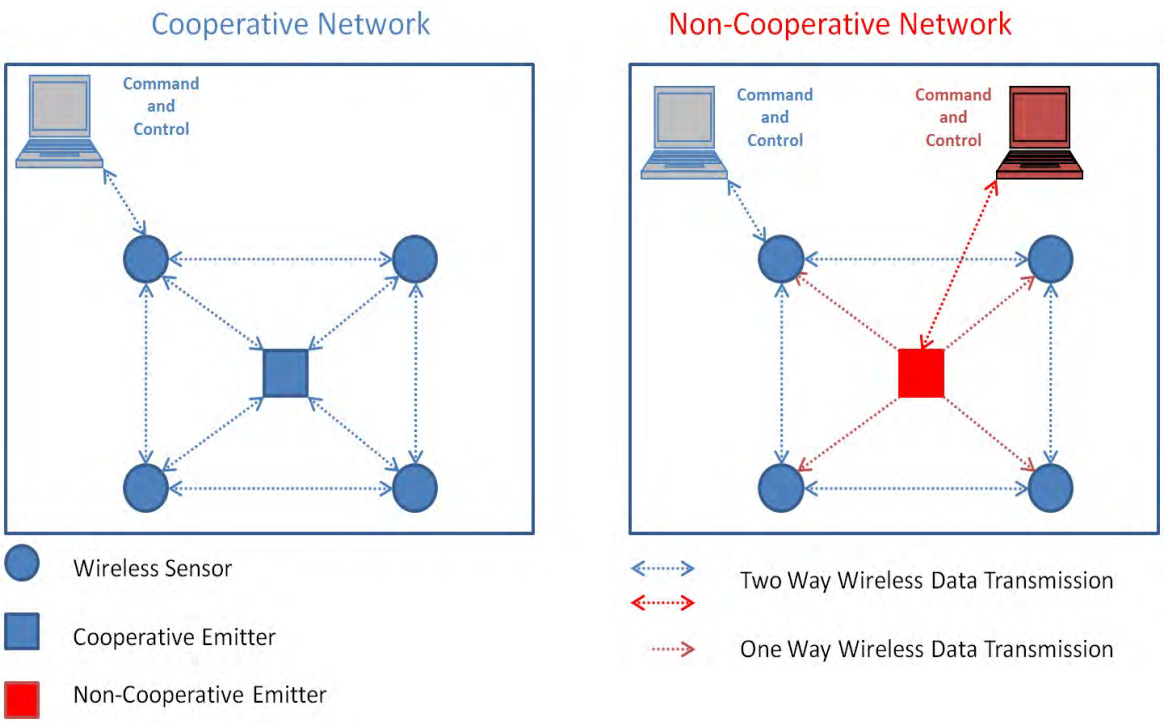

Figure 1.1: Cooperative vs. Non-Cooperative Network.

the emitter is not sharing information. Figure 1.1 shows the differences between a cooperative and non-cooperative network.

1.2 Problem Statement

Cooperative localization networks and measurement techniques are a well understood topic as a large body of literature exists on the topic. Current research for developing a small, low cost, low complexity, and energy efficient NN models is limited. The purpose of this research was to develop a test platform to evaluate the performance of a NN by analyzing measured geolocation data. The sensor mote seen in Figure 1.2 is one of eight sensor motes developed during this research effort to measure a NN's estimated geolocation.

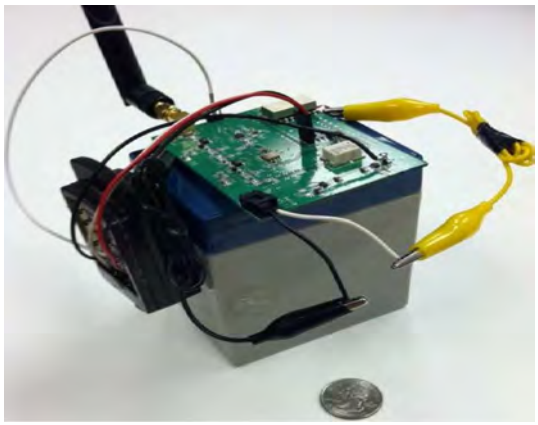

Figure 1.2: Sensor mote that was designed during the research effort that measured a NN's estimated geolocation.

1.3 Scope and Application

This research focused on locating a wireless device in a NN that transmits in the *Industrial, Scientific and Medical* (ISM) radio band of 2.403 GHz to 2.480 GHz. The ISM band is reserved internationally for the use of RF energy for purposes other than licensed communications. Numerous household devices operate in the RF band. Examples of these devices include, baby monitors, garage-door openers, and the newest generation of mobile phones that have incorporated Bluetooth technology [15]. Localization of devices transmitting in the ISM band can be achieved using source localization methods. These source localization methods include measurement-based statistical modeling for *Received Signal Strength* (RSS), *Time of Arrival* (TOA), *Angle of Arrival* (AOA), and *Time Difference of Arrival* (TDOA) measurements. These methods, including advantages and disadvantages, are described in Chapter II [28]. For the purpose of this research, localization is accomplished using RSS measurements. To avoid any confusion, geolocation, localization, and positioning is used interchangeably throughout this thesis.

RSS measurements are achieved in a NN by utilizing a successfully designed *Poor Man's Spectrum Analyzer* (PMSA) circuit board and a *Sun Programmable Objective Technology* (SPOT) device. Spectrum analysis helps analyze electrical signals that are passing through or transmitted by a system or device. By using a spectrum analyzer to

interface with a wireless sensor, detection and analysis of electromagnetic signals over a defined band of frequencies can be made [5]. A SPOT can be used to simulate small wireless transducers, sensors, and other consumer electronic devices [6]. The PMSA interfaced with a SPOT, aids in the detection and analysis of wireless electromagnetic signals.

The original PMSA was designed by Dr. Christopher Anderson of the United States Naval Academy [10]. A majority of the research effort had been focused on modifying, testing and calibrating the PMSA due to pre-existing designs flaws and the fact that the PMSA was not specifically designed to interface with a SPOT mote.

1.4 Research Objectives

The main objective of this research effort is to determine if the functionality of the PMSA and SPOT interface allows the detection and geolocation via RSS of wireless signals over the defined ISM frequency band. *Detection* in this thesis is defined as the sensor's ability to receive and measure the signal's RSS. This objective contains a subset of objectives that must be met to achieve the overall research effort goal. One of these subset objectives is modifying an existing algorithm that measures RSS from a NN and integrates the software into the sensor network. The measured RSS data will then be used to estimate the emitter's location using a *Maximum Likelihood Estimation* (MLE) algorithm. Because the SPOTs are Java programmable embedded devices, the system needs to be robust enough to provide the proper sharing of information between the SPOT and PMSA. Measurements are saved to a text file and then uploaded to *Matrix Laboratory* (MATLAB) where the MLE algorithm is executed.

The last objective is to investigate how the hardware and environmental effects introduce error into the network. These additional errors will impact the accuracy of geolocation measurements. Simulated RSS-based source localization models often ignore these errors and other system limitations.

1.5 Limitations

Specific limitations and assumptions were used to make the research objectives obtainable within time and equipment availability constraints. In this research effort, the emitters of interest were stationary, but a hostile emitter's mobility would normally behave in a random walk manner to avoid detection. The sensor network can be designed to locate multiple emitters. However, this research investigated locating one emitter at a time. The SPOT was not able to measure the PMSA's output voltage fast enough to locate a frequency hopping emitter.

1.6 Equipment Needed

Due to the simple design and low cost of wireless networks that utilize RSS methods, minimum materials and equipment were needed for the end product in this research. All sensors in the network are SPOT and PMSA devices. A lap-top computer connecting a *universal serial bus* (USB) cord to a SPOT base station was used to run the Java and Matlab algorithms. Electronic equipment such as waveform generators were used for the *Initial Operational Test and Evaluation* (IOT&E) of the PMSA [13].

1.7 Motivation

Several factors provide the motivation for this work. One is driven by strong demand and willingness to pay among business wireless subscribers. *Location-Based Services* (LBS) are poised to become a significant growth driver for the US wireless industry. While deployments have been slow to date, carriers have turned their attention to commercial LBS rollouts, including both the addition of location capabilities to existing services, as well as the launch of new applications. It is estimated that LBS will generate annual revenues on the order of US $20+ billion worldwide [8]. Due to annual revenues of that magnitude, research in LBS will continue to be a topic of interest.

A second key motivation factor is to continue research using a low cost and low complexity wireless network. The United States Armed Forces are heavily dependent on GPS-based navigation but are reluctant to embrace GPS fully as the sole location-based technology due to the outdoor and urban limited nature of accurate GPS measurements [28]. Embedding a GPS receiver into wireless devices leads to increased cost, size, and battery consumption. As modern warfare shifts more towards urban operations, it is vital to monitor and track military personnel and enemy combatants where GPS signals are unavailable.

The third motivational factor is the need to monitor and track RF activity near a military installation deployed in a hostile environment. A base's security system could be compromised by an adversary due to the inability to detect and locate malicious activity in a safe and timely manner.

1.8 Organization

Critical points of current knowledge, including substantive findings as well as theoretical and methodological contributions, are presented in Chapter II. Chapter III describes and explains the methodology deployed in this research. This includes detailed descriptions of the NN architecture, PMSA operation, quality control testing, and PMSA IOT&E. Chapter III will includes algorithm development for PMSA/SPOT interface functionality and calibration. Chapter IV provides geolocation measurement analysis using different sensor configurations and emitter characteristics. Finally, Chapter V summarizes the research effort, provides a conclusion, discusses research contributions, and future work.

II. Background

This chapter discusses the critical points of current knowledge, including substantive findings as well as theoretical and methodological contributions.

2.1 Localization

Dramatic advances in RF have made the use of large networks of wireless sensors for a variety of new monitoring and control applications possible. Identifying and locating the origin of wireless signals is a growing area of interest among military and business wireless subscribers [11]. Most localization methods in sensor networks are based on RF signals [28].

Accurate and low-cost sensor localization is a critical requirement for the deployment of large wireless sensor networks in a wide variety of applications. Various application requirements (cost effectiveness, low complexity, energy efficiency, and accuracy) will influence the design of sensor localization systems [25]. The background material presented in this chapter will focus on statistical modeling of CN geolocation and measurement techniques and leverage this information to develop a working system model for locating a NN in Chapter III.

2.2 Measurements Methods

Four common measurement methods use communication signals for localization of wireless devices: RSS, AOA, TOA, and TDOA. These methods use the physical layer of data collected by the sensor and is transmitted by the emitter. The physical layer consists of the basic hardware transmission technologies of a network [16]. TOA, TDOA, and AOA location methods are discussed in this section, as well as multipath, which affects the accuracy of all four measurement methods.

2.2.1 Multipath. The multipath transmission of wireless signals is a major source of error in RSS, TOA, TDOA and AOA geolocation measurement techniques. In wireless location systems, the accurate estimation of TOA, AOA, TDOA, and RSS

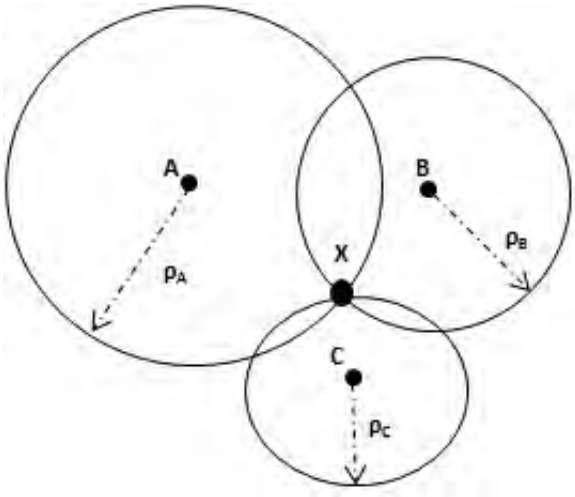

Figure 2.1: Tri-lateration TOA [9].

of the first arriving ray of the multipath channel is vital. Multipath signals occur when there is more than one path for the signal to travel between the transmitter and receiver [25].

Multipath effects include constructive and destructive interference, and phase shifting of the signal. This causes Rayleigh fading [25]. In an urban environment, these multiple paths are typically caused by reflection from buildings and other structures in the environment or even reflections from the atmosphere. Typically the *line-of-sight* (LOS) path from the emitter to the receiver is the strongest and most dominant path, but that is not always the case. If the LOS path is obscured, a multipath signal may become dominant. The impact of these multipath signals depends on many factors such as their power relative to that of the dominant path and range of delays [25].

2.2.2 Time of Arrival. TOA is the measured absolute time at which a signal (RF, acoustic, or other) first arrives at a receiver. The measured TOA is the time of transmission plus a propagation-induced time delay between transmissions and is equal to the transmitter-receiver separation distance divided by a known propagation velocity. TOA data from two devices will narrow a position to two equally probable points. Data from a third device will then resolve the precise position to a single point; this process is called tri-lateration [25]. Fig 2.1 illustrates the concept of

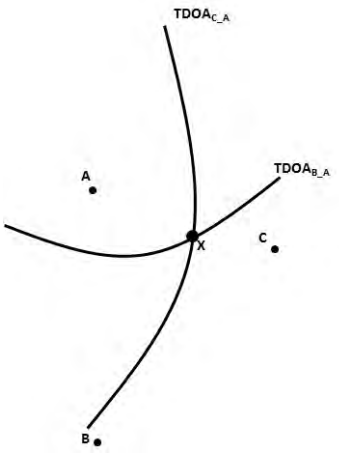

Figure 2.2: TDOA hyperbolic lateration [9].

TOA tri-lateration, where A, B, and C are the receiving sensors. X is the device transmitting the signal and $\rho_{A,B,C}$ are the radial distances to X from each sensor. In some cases, there may be more than one possible solution for the location of an emitter even when using three remote sensors to perform tri-lateration. Adding more sensors will improve the accuracy of localization and is called multi-lateration. Many radio location systems, such as GPS, use TOA [15].

A drawback of the TOA method is the requirement for precise time synchronization of all devices. Given the high propagation speeds, very small discrepancies in time synchronization can result in very large errors in location accuracy. TOA-based positioning solutions are typically challenging in environments where large amounts of multipath, interference, or noise may exist [9].

2.2.3 Time Difference of Arrival. TDOA shares a number of similarities with TOA. TDOA methods use relative time measurements at each receiving sensor in place of absolute time measurements. TDOA does not require the use of a synchronized time source at the point of transmission in order to resolve time stamps and determine location. With TDOA, a transmission of an unknown starting time is received at various receiving sensors, with only the receivers requiring time synchronization. TDOA implementations are rooted upon a mathematical concept known

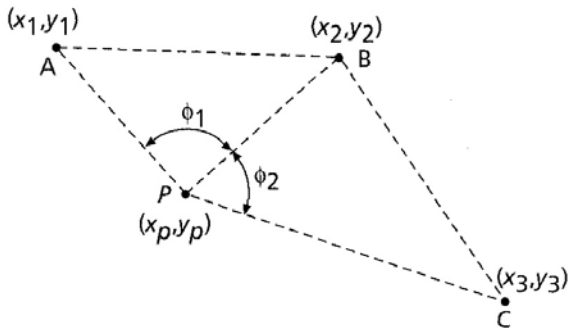

Figure 2.3: Triangulation using three receivers' LOB [26].

as hyperbolic lateration. In this approach, at least three time-synchronized receiving sensors are required. Figure 2.2 illustrates how the intersection of two hyperbolas TDOA_{C-A} and TDOA_{B-A} is used to resolve the position of X.

TDOA-based positioning solutions are also challenged in environments where large amounts of multipath, interference, or noise exist. TDOA methods are highly suitable for large-scale outdoor positioning systems such as GPS and mobile phone tracking [9].

2.2.4 Angle of Arrival. An AOA estimate is made by electronically steering an adaptive phased array antenna in the direction of the arriving emitter's signal. An adaptive phased array antenna is made up of an array of sensors and a real-time adaptive signal processor. A *line-of-bearing* (LOB) is calculated from each AOA estimate and drawn from its corresponding receiver location. These LOBs intersect at the estimated location of the emitter. This method is commonly known as triangulation [23]. An illustration of triangulation is shown in Figure 2.3, in which three fixed receivers (A, B, C) provide LOBs that are used to estimate the location of an emitter (P).

The AOA method allows an emitter's location to be determined with just two receivers, fewer than the TDOA method. Also, no time synchronization between the receivers is required [19, 28]. Both of these advantages reduce the number of receivers needed to measure the AOA of an incoming signal, but extra processor time is needed

to calculate and maintain accurate calibration of the antenna arrays. Relatively large and complex hardware is also needed for AOA estimates [19]. A common drawback that AOA shares with the other methods is its susceptibility to multipath interference. AOA works well in situations with direct LOS, but suffers from decreased accuracy and precision when confronted with signal reflections from surrounding objects [23].

2.3 RSS Research

Positioning techniques based on the RSS have been extensively studied in the literature. RSS is defined as the voltage measured by a receiver's *received signal strength indicator* (RSSI). Often RSS is equivalently reported as the power (i.e., squared magnitude of signal strength) contained in the communication signal measured at the receiver. In CNs, the reported RSS is often only the signal power, as the digital signal can be demodulated and segregated from additive noise [22]. In NNs, RSS may be determined by integrating the observed *Power Spectral Density* (PSD).

RSS measurements are typically inexpensive, simple to implement in hardware, and a popular topic of localization research. Yet, RSS measurements are notoriously unpredictable and often less accurate compared to other localization measurement methods. The more accurate TOA, TDOA and AOA methods are reliable only when LOS signals are dominant. The indoor radio propagation channel is characterized as having severe multipath and low probability for LOS between the transmitter and receiver. Therefore TOA, TDOA, or AOA measurements may not be applicable for an indoor or a dense urban outdoor environment [12].

For RSS geolocation applications, the service area is restricted to the ranging limit in the measurements. In many devices, the ranging limit results in some sensors not reporting beyond some maximum range. In other devices, the RSS is still observed but may exhibit a noise floor at large ranges [22]. The range limit in this research effort partly depended on the gain of the antenna the PMSA used. Shadowing, which is attenuation of a signal due to obstructions (furniture, walls, trees, buildings) also limits accurate RSS measurements. Shadowing causes a signal to pass through or

diffract around the path between the transmitter and receiver. Accounting for these limitations in a design of a wireless network can be cumbersome [25].

A sensor network needs to be carefully designed so that measurement errors of location metrics caused by *non-LOS* (NLOS) propagation can be significantly reduced. The geolocation accuracy of an emitter can be controlled by two design factors, (1) the number and proper placement of sensors, and (2) the geometrical relation among the positions of the sensors and emitters [24].

2.4 Statistical Modeling of CN

Understanding how a CN RSS measurement system operates is useful when characterizing and analyzing a NN. Table 2.1 gives the variables used for statistical modeling and estimation of a CN.

Table 2.1: Variables used for statistical modeling and estimation of CN [21].

Variable	Definition	Dimensionality	Units
S	Number of sensors	Scalar	Unitless
x_0, y_0	Emitter coordinates	Scalar	Unitless
x_s, y_s	Sensor coordinates	Scalar	Unitless
P	Received power vector of all sensors	1 x S	dBm
m_s	Average received power at each sensor	Scalar	dBm
m	Average received power vector of all sensors	1 x S	dBm
σ	Fading channel deviation	Scalar	dBm
I	Identity matrix	S x S	Unitless
Γ_0	Power transmitted	Scalar	mW
P_o	Logarithmic Transmitted Power at some reference distance	Scalar	dBm
η	Path loss exponent	Scalar	Unitless
$d_s(x_0, y_0)$	Path loss component received at each sensor	Scalar	m
w	AWGN	1 x S	dBm
θ	Emitter location	1 x 2	m
$\hat{\theta}$	Estimated emitter location	1 x 2	m

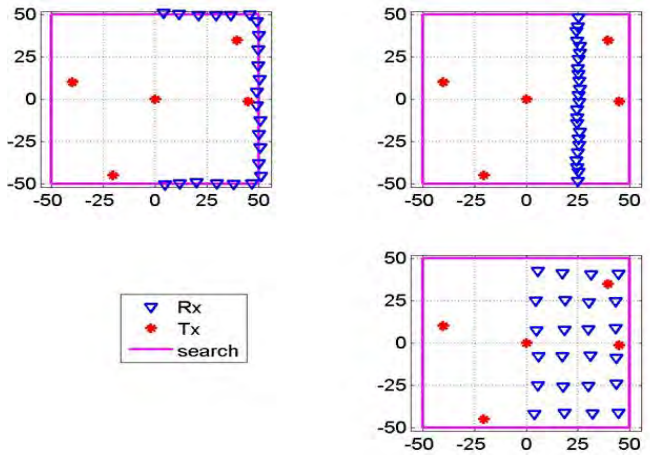

Figure 2.4: Three different sensor configurations are evaluated in determining which of the three was the most efficient in cooperatively locating one emitter (Tx) at five different locations [21].

2.4.1 Statistical Model. Fig 2.4 illustrates a CN RSS system model in which three sensor configurations are evaluated in determining which of the three is the most efficient in cooperatively locating one emitter (Tx) at five different locations. In each configuration, 24 sensors (Rx) are selectively placed [21].

RSS measurements are typically modeled as log-normal, which means the measurements are Gaussian in the *decibel* (dB) scale. (2.1) and (2.2) show the power received at each sensor in vector notation and modeled as a normal distribution [21].

$$\mathbf{P} = [P_1, ..., P_s]^T \tag{2.1}$$

$$\mathbf{P} \sim N(\boldsymbol{m}, \sigma^2 \boldsymbol{I}) \tag{2.2}$$

In free space, a RF signal will decay proportionally with respect to the distance squared. The path loss exponent (η) is not always known, but in free space it is assumed to be 2. The fading standard deviation, σ, is typically in the range 4 dB $\leq \sigma \leq$ 12 dB, with extremes corresponding to deserts and urban canyons, respectively. For this model, it was assumed that $\sigma = 6$ dB. The mean power value received at each sensor s, is given by [21]

$$m_s = \underbrace{10 \cdot \log_{10} \Gamma_0}_{P_0} - \eta \cdot \underbrace{10 \cdot \log_{10} \left(\frac{d_s(x_0, y_0)}{d_0} \right)}_{\overline{d}_s(x_0, y_0)} \tag{2.3}$$

where $s = 1, ..., 24$. The reference power, P_0, is the power that is measured at the reference distance d_0, where $d_0 = 1$ m. For a NN, P_0 is unknown. The P_0 for this model is 20 dB. The locations of the sensors were indicated by (x_s, y_s) and were known; the locations of the emitter were represented by (x_0, y_0) and are unknown [21].

2.4.2 Estimation Theory. In estimation theory, the *Cramér-Rao Lower Bound* (CRLB) expresses a lower bound on the covariance of estimators of a multivariate parameter. The bound further states that the covariance of any unbiased estimator is at least as high as the inverse of the Fisher information. An unbiased estimator which achieves this lower bound is said to be efficient. Such a solution achieves the lowest possible *mean squared error* (MSE) among unbiased methods [17, 25].

Since it is common to model *additive white Gaussian noise* (AWGN) as the impairment to wireless signals, it was worthwhile to derive the CRLB for this general case. The CRLB and Fisher information equations for the CN system model in this subsection were derived for the general case. Equation (2.4) was used to calculate the distance between each sensor and each emitter.

$$d_s(x_0, y_0) = \sqrt{(x_s - x_0)^2 + (y_s - y_0)^2} \tag{2.4}$$

Equation (2.5) represents the linear system model, where P is the power received by the sensor, m_s is from (2.3) and w_s is AWGN with a zero mean and a variance of $\sigma^2 = 36$.

$$P_s = m_s + w_s \tag{2.5}$$

(2.6) gives the conditional probability of $\boldsymbol{P}$ given $\boldsymbol{\theta}$, where $\boldsymbol{\theta} = [x_0, y_0]$.

$$p(\mathbf{P} \mid \boldsymbol{\theta}) = \prod_{s=1}^{S} \frac{1}{\sqrt{2\pi\sigma^2}} e^{\left(\frac{-(\mathbf{P}-\boldsymbol{m}(\boldsymbol{\theta}))^2}{2\sigma^2}\right)} \tag{2.6}$$

(2.7) and (2.8) are the log-likelihood function of (2.6), where Ψ is a constant scalar and does not depend on $\boldsymbol{\theta}$.

$$\begin{aligned} \mathcal{L} &= \ln p(\mathbf{P} \mid \boldsymbol{\theta}) \\ &= \ln \left[\prod_{s=1}^{S} \frac{1}{\sqrt{2\pi\sigma^2}} e^{\left(\frac{-(\mathbf{P}-\boldsymbol{m}(\boldsymbol{\theta}))^2}{2\sigma^2}\right)} \right] \end{aligned} \tag{2.7}$$

$$\mathcal{L} = \psi - \frac{1}{2\sigma^2} \sum_{s=1}^{S} (\mathbf{P} - \boldsymbol{m}(\boldsymbol{\theta}))^2 \tag{2.8}$$

The Fisher information matrix is a $m \times m$ matrix with $[\boldsymbol{J}(\boldsymbol{\theta})]_{ij}$ defined as

$$[\boldsymbol{J}(\boldsymbol{\theta})]_{ij} = -E \left[\frac{d}{d\theta_i} \, ln(p(P \mid \boldsymbol{\theta})) \cdot \frac{d}{d\theta_j} \, ln(p(P \mid \boldsymbol{\theta})) \right] \tag{2.9}$$

By substituting (2.8) into (2.9) the Fisher information reduces to

$$[\boldsymbol{J}(\boldsymbol{\theta})]_{ij} = \frac{-1}{\sigma^2} \cdot E \left[\frac{d\mathcal{L}}{d\theta_i} \cdot \frac{d\mathcal{L}}{d\theta_j} \right] \tag{2.10}$$

By taking the inverse of (2.10), the CRLB is

$$cov(\boldsymbol{\theta}) \geq [\boldsymbol{J}(\boldsymbol{\theta})_{ij}]^{-1} \tag{2.11}$$

2.4.3 Cooperative Network Estimation. Finding the partial derivative and then the log-likelihood function of (2.5) with respect to x_0 and y_0 results in

$$\frac{\partial P_s}{\partial x_0} = \frac{-20 \cdot (x_0 - x_s)}{\ln(10) \cdot d_s^2} \tag{2.12}$$

$$\frac{\partial P_s}{\partial y_0} = \frac{-20 \cdot (y_0 - y_s)}{\ln(10) \cdot d_s^2} \tag{2.13}$$

Using (2.6) and (2.7), the 2×2 Fisher information matrix and CRLB can be found with (2.8) and (2.9)

$$[\boldsymbol{J}(x_0, y_0)]_{ij} = \frac{-1}{\sigma^2} \cdot E \begin{bmatrix} \frac{\partial P^T}{\partial x_0} \cdot \frac{\partial P}{\partial x_0} & \frac{\partial P^T}{\partial x_0} \cdot \frac{\partial P}{\partial y_0} \\ \\ \frac{\partial P^T}{\partial x_0} \cdot \frac{\partial P}{\partial y_0} & \frac{\partial P^T}{\partial y_0} \cdot \frac{\partial P}{\partial y_0} \end{bmatrix} \tag{2.14}$$

$$cov(\boldsymbol{\theta}) \geq [\boldsymbol{J}(x_0, y_0)]_{ij}^{-1} \tag{2.15}$$

where $cov(\boldsymbol{\theta})$ is the CRLB of the unbiased estimator. Next deriving the MLE will give an estimate of the emitter location. This was done by finding the values of $\boldsymbol{\theta}$ that maximize (2.7) by setting the gradient of (2.8) with respect to $\boldsymbol{\theta}$ equal to 0. This was equivalent to finding a maximum by taking the derivative and setting it equal to 0.

$$\nabla_\theta L = 0 = \nabla_\theta \left(\psi - ||\mathbf{P} - \boldsymbol{m}(\boldsymbol{\theta})||^2\right) \tag{2.16}$$

When finding the argument that minimizes (2.16), no closed form solution exists. Therefore, the MLE is

$$\hat{\boldsymbol{\theta}} = argmin_{\boldsymbol{\theta}} \|\boldsymbol{P} - \boldsymbol{m}(\boldsymbol{\theta})\| \tag{2.17}$$

The bias between $\hat{\boldsymbol{\theta}}$ and $\boldsymbol{\theta}$ is calculated using (2.18)

$$\boldsymbol{bias} = E[\hat{\boldsymbol{\theta}} - \boldsymbol{\theta}] \tag{2.18}$$

and the covariance matrix is calculated using a built in algorithm in the simulations. Both calculations are averaged over 100 trials.

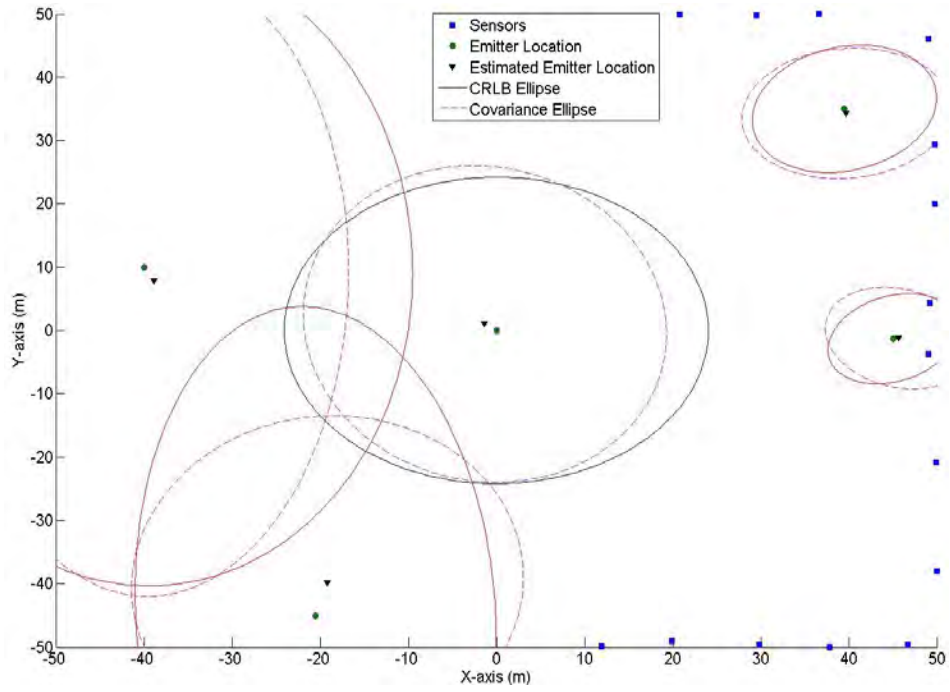

Figure 2.5: Sensor Config 1 - Actual vs. Estimated emitter location.

The MLE is one of many techniques used to quantify the difference between the values implied by the estimator and the true values of the quantity being estimated. MSE is a risk function, corresponding to the expected value of the squared error. MSE measures the average of the squares of the errors. The error is the amount by which the value implied by the estimator differs from the quantity to be estimated. The error results from noise in the observations and is due to the estimator not accounting for information that could produce a more accurate estimate. By calculating the *root MSE* (RMSE), a good measure of precision of the parameter estimated is obtained [20]. The RMSE was calculated using (2.19)

$$RMSE = \sqrt{\frac{1}{M}\sum_{m=1}^{M}(\hat{\boldsymbol{\theta}} - \boldsymbol{\theta})(\hat{\boldsymbol{\theta}} - \boldsymbol{\theta})} \tag{2.19}$$

The estimated emitter location ($\hat{\boldsymbol{\theta}}$), actual emitter location ($\boldsymbol{\theta}$), CRLB, and covariance error ellipses at 90% confidence intervals are plotted for all three sensor configurations. The plots illustrated in Figures 2.5-2.7 are averaged over 100 trials.

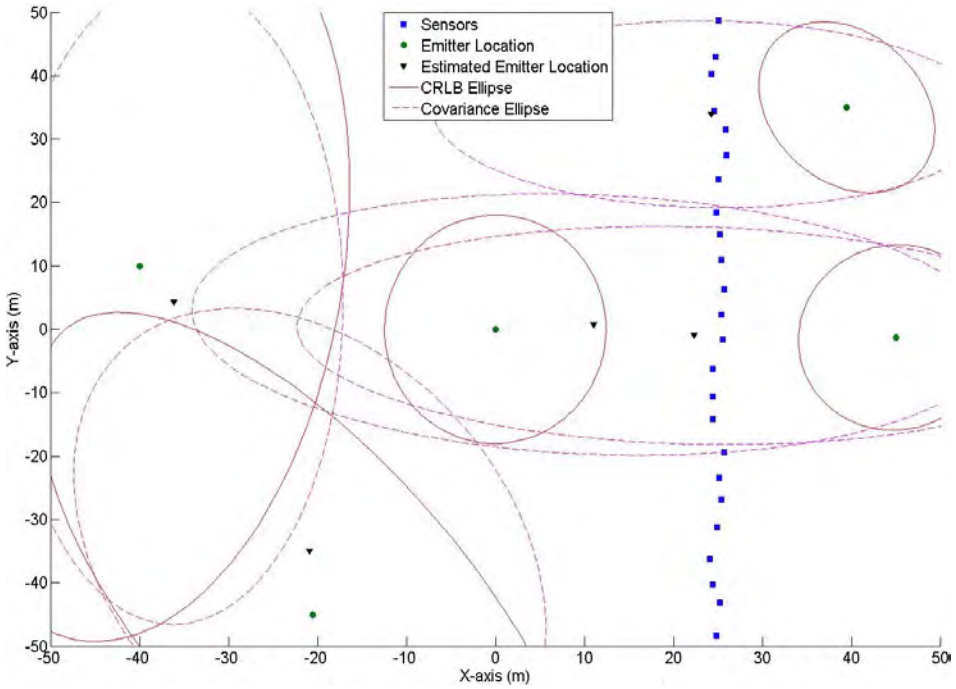

Figure 2.6: Sensor Config 2 - Actual vs. Estimated emitter location.

The CRLB ellipse is determined by the MSE and is centered at the true emitter location. The covariance ellipse is centered at the estimated location. The simulated measurements for $\hat{\boldsymbol{\theta}}$, $\boldsymbol{\theta}$, Root CRLB and RMSE are shown in Table 2.2. The Root CRLB and RMSE differ from one another because the CRLB calculation is for an unbiased estimator. Table 2.2 shows that by having a larger RMSE value will result in larger error ellipses. These values are consistent with the plots in Figures 2.5-2.7.

The sensor network in Figure 2.5 provided the most accurate estimated emitter localization measurements than the other two sensor configurations. This was determined by averaging each sensor configuration's bias and RMSE measurements and then selecting the configuration that had the lowest averaged values. Intuitively, sensor configuration 2 had the poorest geolocation performance of the three configurations. This was a result of the sensors being vertically stacked on top of each other and not as evenly spaced as the other two configurations.

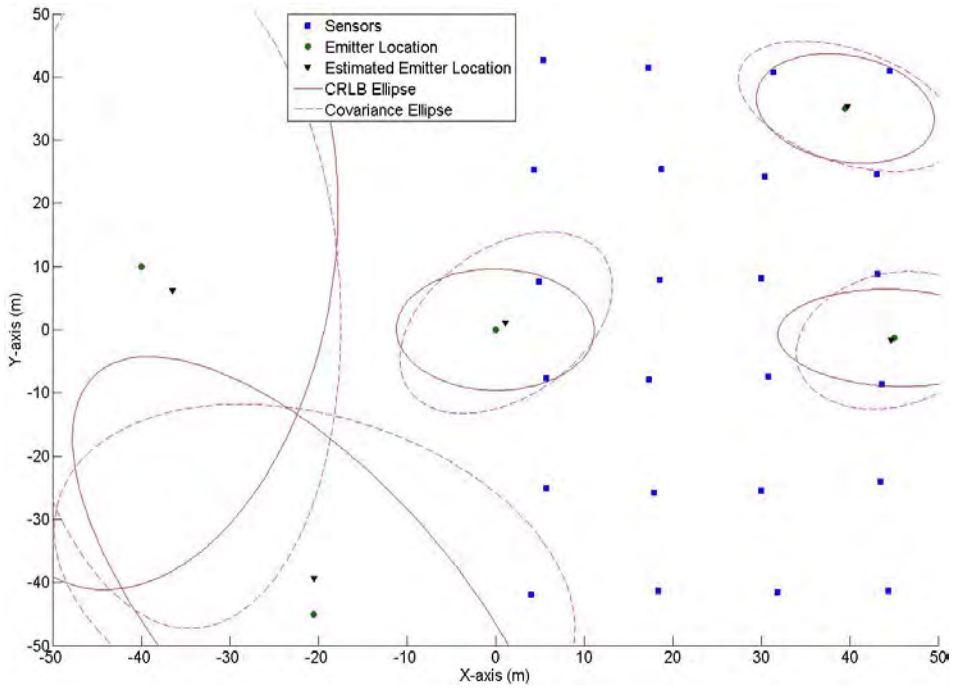

Figure 2.7: Sensor Config 3 - Actual vs. Estimated emitter location

2.5 Error Ellipses

The covariance error ellipse changes its shape as a function of the covariance matrix, the eigenvalues, and the correlation coefficient. The set of all possible covariances defines a covariance matrix, denoted V_{ij}. The diagonal elements of V_{ij} are the variances of the individual variables and are also called the eigenvalues. While the off-diagonal elements are always equal and are related to the correlation coefficients. (2.20) is the general case n×n covariance matrix [17]

$$V_{ij} = \begin{bmatrix} \sigma_1^2 & \rho_{12}\sigma_1\sigma_2 & \cdots & \rho_{1n}\sigma_1\sigma_n \\ \rho_{21}\sigma_1\sigma_n & \sigma_2^2 & \cdots & \rho_{2n}\sigma_2\sigma_n \\ \vdots & \vdots & \ddots & \vdots \\ \rho_{n1}\sigma_1\sigma_n & \rho_{n2}\sigma_2\sigma_n & \cdots & \sigma_n^2 \end{bmatrix} \tag{2.20}$$

where σ^2 is the variance and ρ is the correlation coefficient. The covariance ellipses plotted throughout this thesis are from a 2×2 covariance matrix. An ellipse is circular when both variances are equal and the correlation coefficients are equal to zero (off-

Table 2.2: Emitter locations (x_0, y_0), Root CRLB and RMSE (m)

		Hostile Emitter Data				
	Actual	(0.0, 0.0)	(-40.0, 10.0)	(39.5, 35.0)	(45.0, 1.3)	(-20.5, 45.1)
1	Estimate	(-1.3, 1.0)	(-38.9, 7.8)	(39.7, 34.3)	(45.7, -1.2)	(-19.2, -39.8)
	Root CRLB	15.9	27.4	6.8	4.8	24.7
	RMSE	15.1	25.4	7.3	5.4	16.1
2	Estimate	(11.1, 0.7)	(-36.1, 4.3)	(24.3, 33.9)	(22.4, -1.0)	(-20.9, -35.0)
	Root CRLB	10.2	29.7	7.8	8.5	26.5
	RMSE	23.1	25.3	16.1	22.3	21.7
3	Estimate	(1.2, 1.1)	(-36.4, 6.2)	(39.8, 35.4)	(44.7, -1.7)	(-20.4, -39.4)
	Root CRLB	6.9	26.0	6.2	7.1	22.9
	RMSE	8.7	26.4	7.5	7.1	18.8

diagonal elements are zero). As seen in Figure 2.8, the following changes to the elements of the covariance matrix affect the size of a circular shaped ellipse:

1 The ellipse will increase horizontally when σ_1^2 increases.

2 The ellipse will increase vertically when σ_2^2 increases.

3 As the correlation coefficient increases from zero (off-diagonal elements increase), the ellipse will become narrower and the top of the ellipse will be pointing to the right.

4 As the correlation coefficient decreases from zero (off-diagonal elements decrease), the ellipse will become narrower and the top of the ellipse will be pointing to the left.

The CRLB error ellipse is determined by the CRLB matrix. The CRLB ellipses plotted throughout this thesis are from a 2×2 CRLB matrix and are a function of the MSE. The RMSE is calculated by squaring the diagonal elements of the CRLB

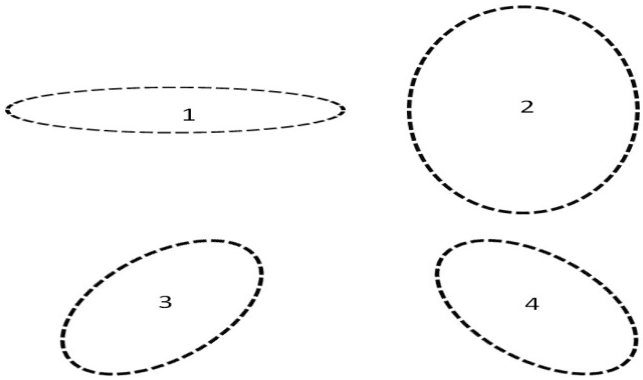

Figure 2.8: Changes to the elements of the covariance matrix and how it affects the size of the ellipse.

matrix, adding the squared elements and then taking the square root. Similar to the covariance ellipse, the off-diagonal elements are always equal and the size and shape of the CRLB ellipse was determined by varying the elements inside the matrix [17].

2.6 Chapter Summary

This chapter provided critical points of current knowledge including substantive findings as well as theoretical and methodological contributions. An overview into the application of cooperative geolocation of an emitter in three wireless sensor network configurations was also provided. A measurement based statistical model of RSS was presented to generate performance bounds and perform localization calculations. At the end of Section 2.3 it was mentioned that the location accuracy of an emitter can be controlled by two design factors: (1) the number and proper placement of sensors, and (2) the geometrical relation among the positions of the sensors and emitters. The relevance of these design factors was verified and validated in Figures 2.5-2.7. The critical points and knowledge gained from the simulations and analytical analyses of the CNs presented in Section 2.4 were leveraged in gaining a fundamental understanding of how a NN operates.

III. Research Methodology

This chapter will detail the methodology used to design and test the hardware-software integration of the PMSA and SPOT for non-cooperative geolocation. This chapter will include a detailed explanation of the following topics:

1 System model of the major components in the NN

2 PMSA operation

3 PMSA *quality control* (QC) testing

4 PMSA IOT&E

5 *Low rate initial production* (LRIP)

6 *Full rate production decision review* (FRPDR)

3.1 NN System Model Architecture

The proposed NN system model consists of three major components:

- SPOT/PMSA sensor network
- Non-cooperative emitter
- *Command and Control* (C2) center

3.1.1 Sensor Devices. A SPOT is an open wireless sensor network mote developed by Sun Microsystems. To be considered as an open wireless sensor, the sensor must provide freely downloadable source code and make available a full description of the hardware. It should be possible for anyone to replicate the device without any special permission. The SPOT motes consist of three components: (1) a demo sensor board, (2) a processor board, and (3) a battery. The SPOT device uses Java technology to up-level programming. Developers can write a program in Java, load it on a wireless sensor device, run it, debug it, as well as access low-level mechanisms with standard Java integrated development environments. What distinguishes the SPOT

Figure 3.1: SPOT base station, two SPOTs and PMSA (left to right).

mote from comparable devices is that it runs a Java micro edition virtual machine called Squawk directly on the processor without an operating system. The SPOT's use of Java device drivers is particularly remarkable, as Java is known for its ability to be hardware-independent [6].

Using the PMSA to interface with a SPOT, visual detection and analysis of RF signals outside a sensor network are made. The SPOT and PMSA interface are used to simulate the sensors in a NN.

3.1.2 Non-Cooperative Transmitting Devices. The second key component of a NN is the transmitter. A non-cooperative RF emitting device iss operated and controlled outside of the sensor network. There is little or no *a priori* knowledge of emitter properties for the sensor network to exploit WND. However, emitter properties such as transmission power and location are known to the network designer to aid in PMSA/SPOT calibration and geolocation estimation analysis.

3.1.3 Command and Control Center. The controlling operations, algorithm implementation and data reporting from the sensor network are performed in the C2 center. The C2 center consists of a SPOT base station and laptop computer. The SPOT base station allows applications to run on a host computer to interact with applications running on SPOT motes. The base station unit is recognizably smaller

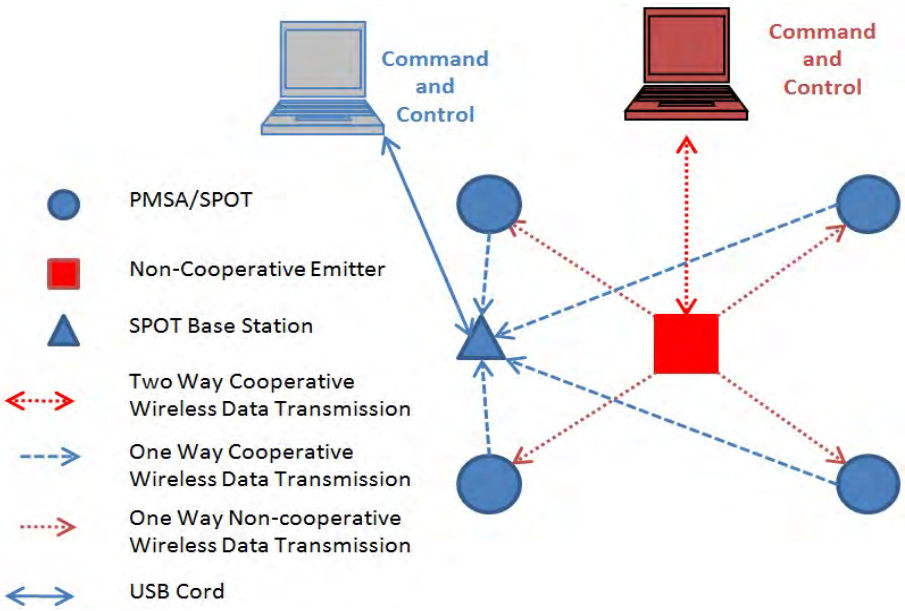

Figure 3.2: System components and connections.

than a SPOT mote and communicates wirelessly with the SPOT, which then streams the data via a USB connection to the host computer. Figure 3.1 shows a SPOT base station unit, two SPOT motes and a PMSA. Figure 3.2 is a sketch of system components and connections. This figure shows four PMSA/SPOT motes, the C2 center (laptop and SPOT base station) and a non-cooperative network. Figure 3.2 shows only how the system components are connected to one another. The figure is not an accurate representation of the quantity and placement of these components used during this research effort.

Besides a base station mote being present, Figure 3.2 differs from Figure 1.1 in that the PMSA/SPOT motes do not wirelessly communicate back and forth with each other, but solely with the base station. Because of the lack of communication between the PMSA/SPOT motes, the sensor network was not configured to multi-hop data back to the C2 center. Hopping is a capability that all SPOT devices can have if programmed correctly. However for simplicity, the PMSA/SPOT motes do not multi-hop information as this operation was not necessary to achieve the research objectives.

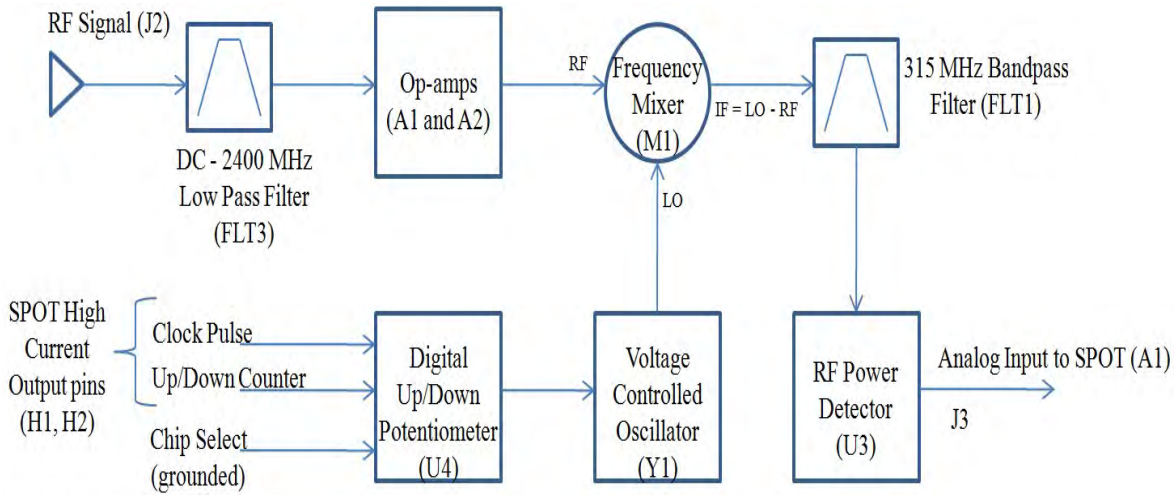

Figure 3.3: PMSA block diagram.

3.2 PMSA Operation

Before PMSA testing is discussed, it is fundamental to understand how the major electronic components of the PMSA operate. The major components in any spectrum analyzer are [5]:

- RF Input Antenna
- Amplifier
- Frequency Mixer
- *Bandpass* (BP) Filters
- Power Detector
- *Voltage Controlled Oscillator* (VCO)
- Digital Potentiometer

Figure 3.3 shows a block diagram of the major components of the PMSA while Figures A.1 and A.2 show the electrical schematic of the original (ver.1) and redesigned PMSA (ver.2).

A RF antenna connected to the port of J2 receives a signal in the ISM frequency band. The received signal is sent through a low pass filter (FLT3) where the

signal experiences slight power loss due to filter coloration. The signal is amplified by *operational amplifiers* (Op-amps), A1 and A2. The gain at the output of the Op-amps is positive, and the actual value depends on the input signal's frequency, the surrounding environment temperature and input power.

The amplified filtered signal is sent to one of the input ports of the mixer (M1). M1 is a three-port device that converts a signal from one frequency to another. The input signal is applied to one of the input ports, and the output of the VCO is applied to the other. By definition, a mixer is a non-linear device, meaning there are frequencies at the output that are not present at the input. The output frequencies that are produced by M1 are the original input signals (labeled RF and LO in Figures 3.2, A.1 and A.2), plus the sum and difference frequencies of these two signals. It is the difference frequency that is of interest. This signal is called the *intermediate frequency* (IF) signal. The mixer in the PMSA utilizes frequency division multiple access so that multiple users (signals) of different frequencies can be detected due to the individual allocations of the frequency band being used [3]. More than one user can occupy an individual sub-band, but only one can be detected at a time.

The IF signal is filtered by a BP filter with a center frequency of 315 MHz and a 3 dB bandwidth of 600 KHz. When 314.7 MHz $\leq$ IF signal $\leq$ 315.3 MHz, the filtered IF signal is passed to the power detector. Y1 is an oscillator controlled by the voltage output of the digital up/down potentiometer (U4). The frequency of oscillation is varied by the input DC voltage. By design, the desired voltage to the input of Y1 should be approximately 4.17 - 4.9 V so that the VCO can tune the IF signal to within the 3 dB bandwidth of the BP filter [7].

U4 is a 128-position digitally controlled *variable resistor* (VR) device. Changing the VR settings is accomplished by pulsing the *clock pin* (CLK) while the *chip select* (CS) is active low. The direction of the increment is controlled by the *up/down* (U/D) control pin. When the wiper (W1) hits the end of the VR, terminals A1 (Pin 3) or B1 (Pin 6), additional pulses to the CLK no longer change the wiper setting until the

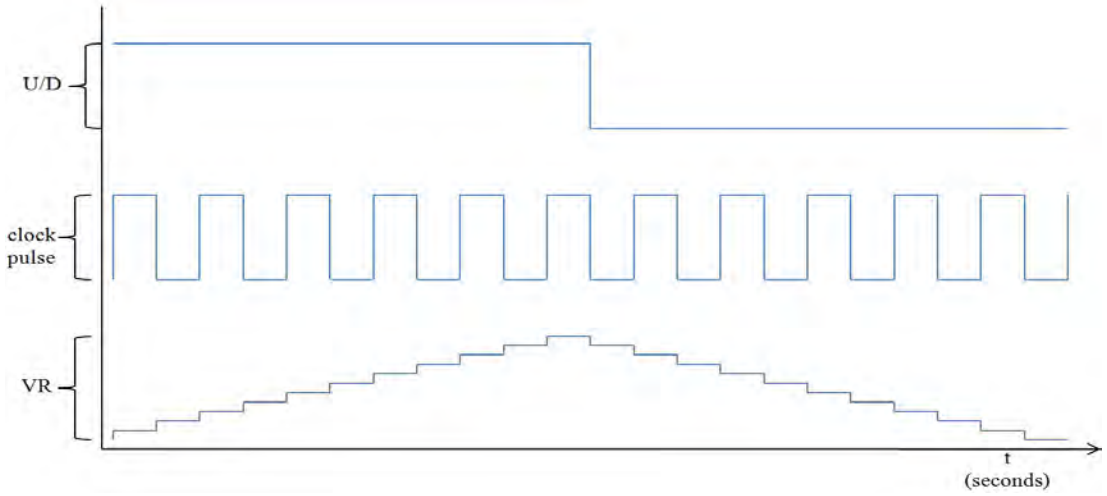

Figure 3.4: Direction of the VR's wiper setting increment due to U/D logic during clock pulses.

U/D pin changes states. W1, A1 and B1 are also seen in Figures A.1 and A.2. The wiper position is immediately decoded by the wiper decode logic changing the wiper resistance. When the PMSA is interfaced with the SPOT the high current/voltage input/output pins of the SPOT will provide the clock pulse and change the U/D control pin to active high or low to increment or decrement the output voltage of U4 [2]. Figure 3.4 (not drawn to scale) shows that the direction of the VR's wiper setting increment during clock pulses is controlled by the U/D control pin.

The PMSA covers the frequency spectrum of approximately 2.403 GHz - 2.48 GHz. The 77 MHz difference is divided into 128 sub-bands of width of approximately 600 KHz. Since U4 is a 128-position digitally controlled VR, there are 128 frequency values. Changing VR should provide the desired output voltage stated above to tune the frequency output of Y1 to the desired frequency band to achieve an IF signal in the 314.7 MHz to 315.3 MHz range [2].

U3 is a logarithmic RF power detector. The power detector consists of cascaded limiting amplifiers and RF detectors. The output current from every RF detector is combined and low-pass filtered before applied to the output buffer amplifier. As a result, the final DC output voltage approximates the logarithm of the amplitude of the input signal. The output at J3 must be in the range of 0 to 3 V as this will be

the input to the analog input pin (A1) of the SPOT. If the output voltage should fall outside this range, there is potential to damage the SPOT's *analog-to-digital converter* (ADC) [1].

3.3 PMSA Quality Control Testing

Quality Control emphasizes testing of the PMSA to uncover defects, unintentional performance degradation and restrictions due to the fabrication process or circuit design error. During the QC process, numerous design flaws were found with the PMSA ver.1 design that either left the PMSA inoperable or limited its performance. Even though the PMSA ver.1 was not specifically built for this research, any modifications to the board are defined as a design error or flaw due to ver.1 being unable to meet the research objectives. For visual comparison between the original design and the redesigned PMSA, see Figures A.1 and A.2.

Before power was applied to the PMSA, the first modification was to add three 0.01 μF capacitors between L2/R5, R6/A2 input, and L1/R7. Cutting the copper traces between these components and soldering the capacitors onto the board achieved this modification. The capacitors were added to block out the DC component of the RF input signal.

The ENBL (Pin 1) on U3 was open (no voltage applied). An applied voltage above 1 V will activate the bias for the chip, turning it on. For an applied voltage below 0.3 V, the chip will be shut down (disabled). Since U3 was not turned on, there was no possibility to collect usable data from the power detector's output (J3). To correct this error, a copper wire was soldered from the ENBL pin to U3's V_{CC} [1].

U4 needed several corrections. Due to the model of the chip, the design errors present and the surrounding components of U4, the best solution was to place a drop-in pin model of U4 into a bread board to troubleshoot. Once the drop-in pin U4 and its surrounding components were placed on the bread board, the trace between U4 pin 5 and the input to Y1 on the PMSA was cut. A copper wire inserted into the

bread boarded U4 pin 5 and then soldered to the input of Y1 on the PMSA. During this redesign process, the location and type of design flaws became more apparent. Per chip design specification, pin 4 had to be grounded, but was not. Since CS (pin 7) needs a logic low for U4 to be turned on, it also provided the ground connection for the clock pulse and the voltage applied to the U/D pin. Grounding CS would simplify the PMSA design by using a 3-pin connection header instead of the 6-pin header (J1). Since a toggle switch was not used to provide the clock pulse to the CLK, R15, R16, and the 5 V input were removed. The 6.5 V input at pin 3 was changed to 4.90 V by adding a voltage divider network. Per chip design specifications, voltage greater than 5.5 V caused permanent damage to the chip. The reason for the damage was the VR exceeded its maximum current rating of 5 mA. Another reason for changing pin 3 input voltage was the maximum output voltage desired at the input of the VCO was also 4.90 V. This is because U4 generates an output voltage proportional to the input voltage applied to the terminals A1 and B1 [2].

The VCO tunes the frequency of the LO signal to the corresponding input voltage. An input voltage of 4.90 V accounted for a frequency of approximately 2.48 GHz, which was just inside the top end of the ISM band [7]. To ensure the VCO tuned the LO frequency to include the bottom of the ISM spectrum while also maintaining the smallest possible voltage range U4 increments/decrements to, 4.17 V was applied to B1. In order to step down the 6.5 V that was applied to B1, a voltage divider network (R2 and R17) was included in the original design. However, R2 and R17 values were incorrect, as these resistors did not step the voltage down to 4.17 V. By applying Ohm's Law, the relationship between the input voltage, 6.5 V, and the output voltage, 4.17 V, was found. The voltage divider network and Ohm's Law are seen in Figure 3.5 and equation (3.1).

$$B1 = \left(\frac{R17}{R17 + R2}\right) 6.5V \tag{3.1}$$

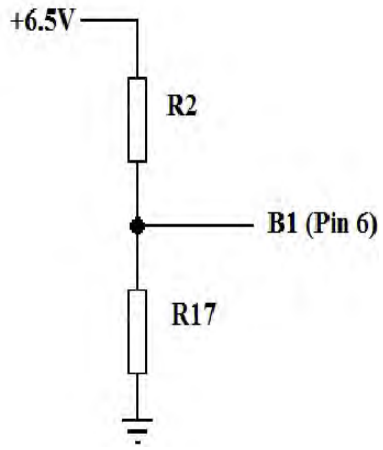

Figure 3.5: Voltage divider network for terminal B1.

In using (3.1), the voltage at the terminal B1 was approximately 3.97 V in the original PMSA design. This value was lower than the desired 4.17 V. The resistors in the voltage divider network were then changed to $R17 = 417\ \Omega$ and $R2 = 233\ \Omega$. The bread boarded PMSA is seen in Figure 3.6. There were a few other design adjustments that were needed to the PMSA when interfaced with a SPOT. These adjustments are not shown in Figure 3.6 since PMSA/SPOT design modifications are covered in Section 3.5.3. The summary of the PMSA design error and corrections are listed in Table 3.1.

3.4 PMSA Initial Operational Test and Evaluation

Part of the main research objective described in Chapter I is for the SPOT to:

- Provide a clock pulse to U4 on the PMSA
- Increment and decrement U4's U/D pin
- Measure U3's output voltage (J3)

Once design modifications were made to the PMSA, it was ready for IOT&E [13]. During the IOT&E phase, the SPOT was not interfaced with the PMSA. To mimic the services of the SPOT listed above, the PMSA used electronic equipment that consisted of:

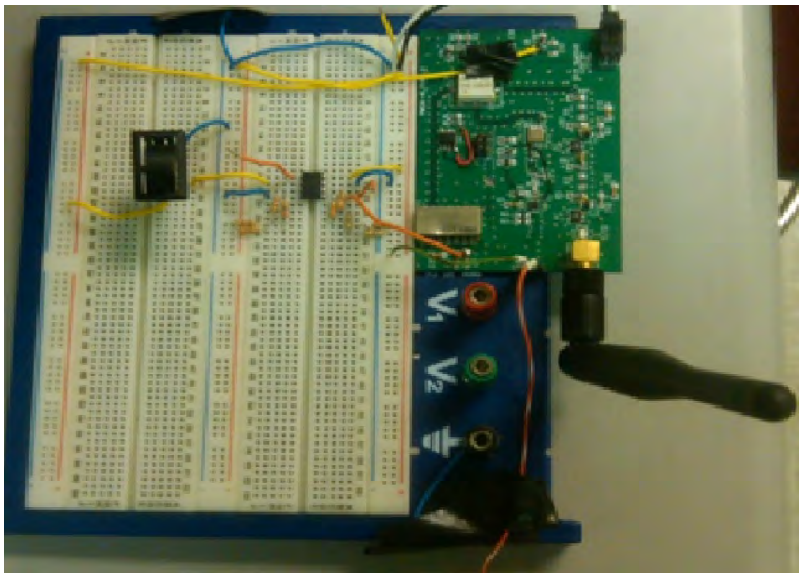

Figure 3.6: PMSA bread board

- Square/pulse waveform generator
- Dual DC regulated power supply
- Voltmeter

The square/pulse waveform generator was used to clock the PMSA by providing a 5.0 V peak-to-peak signal. The pulse signal had a 500 μsec pulse duration and a frequency of 60 Hz. The dual DC regulated power supply was used to provide 6.5 V to the PMSA and 5.0 V applied to a switch. The switch was also connected to ground to increment/decrement the frequency spectrum by applying a high/low voltage setting to U/D pin. A RF wireless signal generator acted as the non-cooperative emitter. During IOT&E, the adjustable RF signal generator output was set between -26 dB to 14 dB with frequency range of 2.403 GHz to 2.480 GHz. The voltmeter was used to measure J3's output voltage. The electronic equipment and the bread boarded PMSA make up the PMSA test bed that is seen in Figure 3.7.

In-depth testing and calibration was not performed on the PMSA test bed. The purpose of the PMSA test bed was to evaluate if the redesigned PMSA is operational, as described in Section 3.2. A 2.40 GHz to 2.50 GHz, 4 dB omni-directional antenna

Table 3.1: Summary of PMSA ver.1 QC test results

Design modifications	Correction	Justification
6-pin connection header (J1)	Change to 3-pin connection header	Simplifies design
5V input to CLK, U/D pin, R15 and R16	Remove	Not using a toggle switch to clock U4
U4 Pin 4 not grounded	Ground pin 4	Per chip specifications
Incorrect R2 and R17 values	R2 = 233 Ω R17 = 417 Ω	Desired lower limit voltage value for VCO
Missing three 0.01 μF capacitors	Add capacitors between L2/R5, R6/A2 input and L1/R7	Filter's out DC component of RF input signal
U3 disabled	Connect ENBL (Pin 1) to +5V	Per chip specifications
6.5V to U3 pin 3	Change to 4.90 V by adding voltage divider	Voltage $\geq$ 5.5V causes irreparable damage to U3

with a RP-SMA plug connector was connected to the PMSA to receive a RF signal. As U4 was clocked going up and down the frequency spectrum, the voltage measured at J3 would spike when the IF signal was between 314.7 MHz and 315.3 MHz. When the IF signal was outside these frequency values, a voltage floor was measured. As U4 would clock up the spectrum, there was a small gain of the voltage floor of approximately 110 mV. The voltage floor values seen in the ISM band were approximately 0.65 V to 0.76 V. The cause of the voltage floor gain is from the frequency gain of A1 and A2. The voltage spike would range from approximately 0.76 V to 1.50 V. The magnitude of the spike depended on the distance the emitter was from the bread boarded PMSA and the amplitude of the transmitted signal. The term voltage and measurement floor are used interchangeably throughout this thesis.

Figure 3.8 shows the PMSA output voltage vs. transmitted power from 1, 2, 5 and 10 ft away. There are nine data points shown for every transmitted power measurement. The nine data points came from adjusting the signal generator's frequency from 2.403 GHz to 2.480 GHz, incremented in 8.55 MHz step. It was determined that

Figure 3.7: PMSA test bed

the small gain of the voltage floor had no effect on how much the voltage spike would peak during the PMSA detection of the RF signal. According to the PMSA operation in Section 3.2, the results of Figure 3.8 verified and validated the successful redesign of the PMSA and proper set up of the test bed.

3.5 PMSA/SPOT Low Rate Initial Production

The LRIP for this research effort is defined as the integration, test and calibration of system components in order to achieve a working prototype of a sensor mote. At the conclusion of LRIP, the system had been tested over some protracted amount of time in order to gain a reasonable degree of confidence as to whether the system will achieve the research objectives before final production and system performance evaluation began [13]. The following work elements were accomplished in the LRIP phase:

- Interface PMSA/SPOT hardware

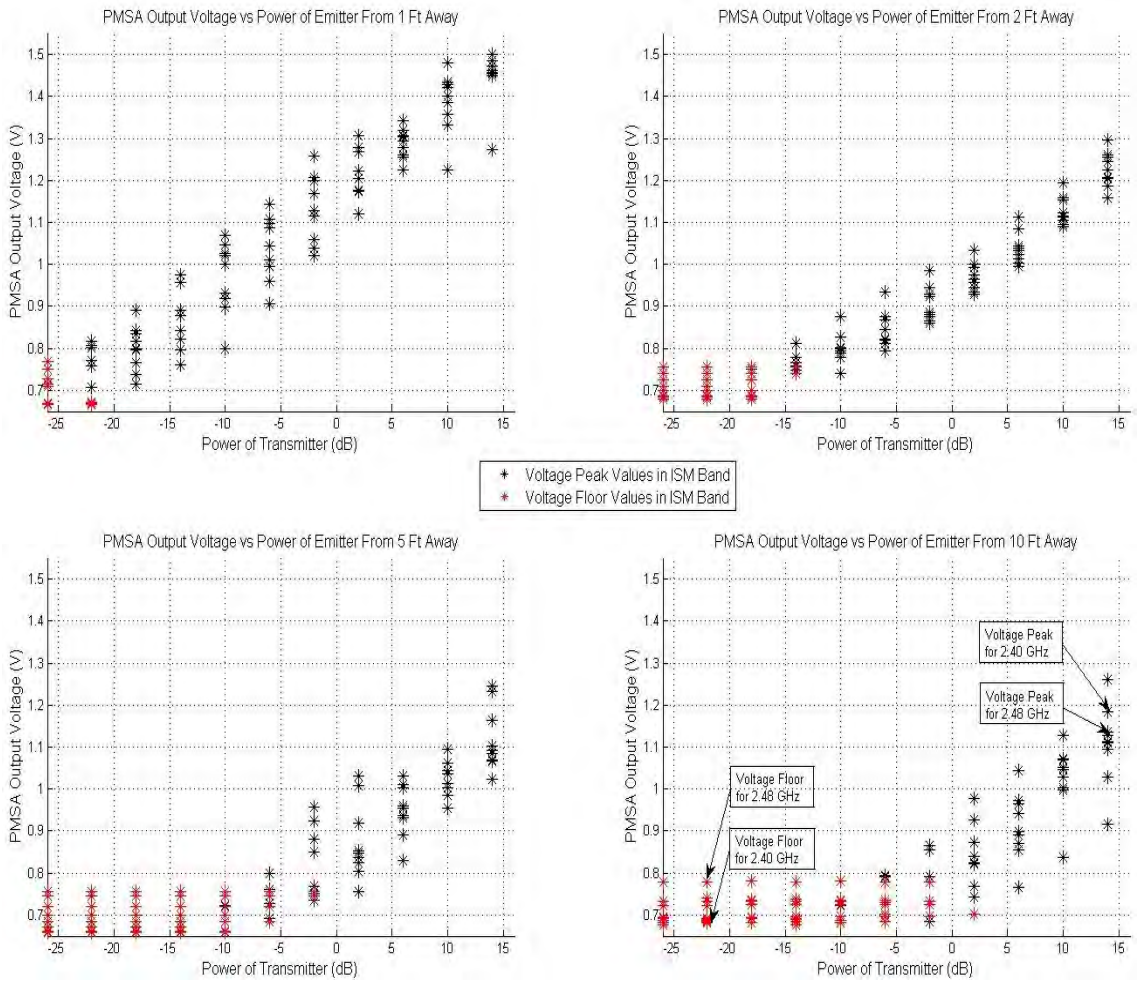

Figure 3.8: PMSA output voltage vs. power of emitter from 1, 2, 5, and 10 ft away.

- PMSA/SPOT RSS algorithm development
- PMSA/SPOT QC testing
- PMSA/SPOT calibration

3.5.1 Interface PMSA/SPOT Hardware. The SPOT was interfaced with the PMSA through the SPOT's demo sensor board. The demo sensor board pictured in Figure 3.9 has a 20-pin I/O connector. It was through this connector that the SPOT and the PMSA were wired together. The following pins on the demo sensor board were used for the SPOT/PMSA interface:

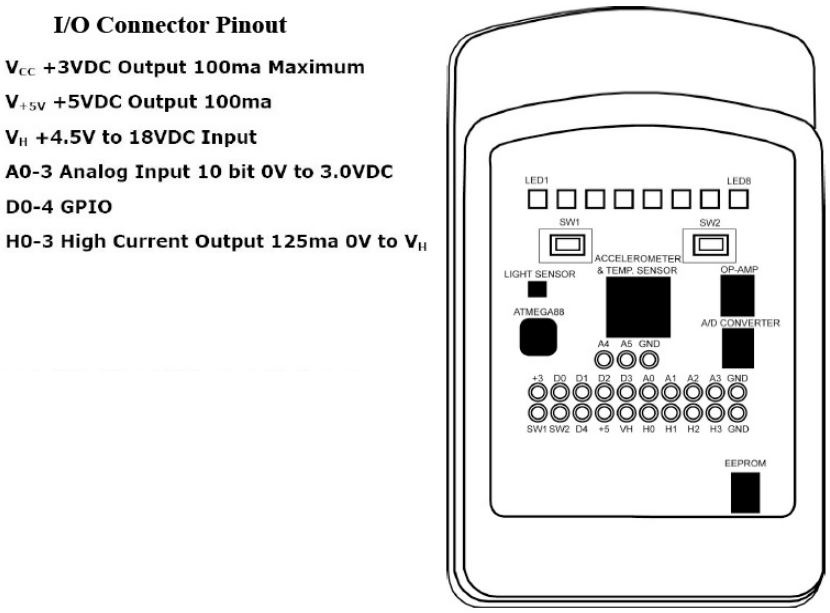

Figure 3.9: SPOT demo sensor board (permission given by Oracle to use figure) [29].

- V_H - inputs voltage from outside power source
- H1 - voltage from V_H provided clock pulse for U4
- H2 - voltage from V_H provided high/low voltage to U/D pin on U4
- GND - ground connection
- A1 - inputs J3 measurements

The SPOT did not power the PMSA. The SPOT did not output enough current to drive the PMSA circuitry and the PMSA was designed to turn on when 6.5 V was applied. There was no pin on the demo sensor board that can power the PMSA unless an external power source was applied to it. The high current/voltage I/O H0-H3 pins were able to output a voltage when an external power source was applied to the V_H pin. The external power source came from soldering a wire at the output of the 6.5 voltage regulator, U5 on the PMSA to the V_H pin on the SPOT demo sensor board. The digital output pins, D0-D3 were initially considered for the clock pulse and high/low voltage for the U/D pin on U4. However, these pins were not able to output enough current for the clock pulse to increment or decrement through

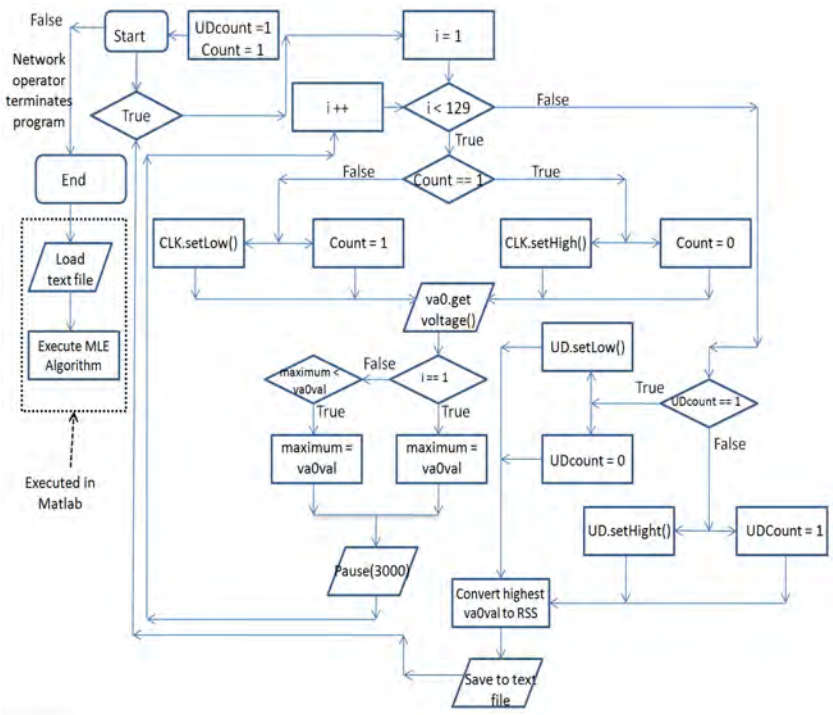

Figure 3.10: SPOT RSS measurement algorithm flow chart.

the frequency spectrum. It was mentioned in Section 3.2 that DC output voltage of the PMSA (J3) must be in the range of 0 to 3 V as it was the input to the analog input pin (A1) on the SPOT. If the output voltage fell outside the 0-3 V range, there was potential to damage the SPOT's ADC. Any one of the analog pins A0-A3 could have been used as J3's input. An algorithm was developed to properly turn on A1, H1, and H2 to input and output the desired voltage. This algorithm programed the SPOT to:

- Clock U4 to go up and down the frequency spectrum
- Measure the PMSA output voltage
- Convert the peak voltage value to a RSS measurement
- Estimate the frequency of transmitting device

3.5.2 PMSA/SPOT RSS Measurement Algorithm Development. Figure 3.10 is a flow chart of the Java embedded SPOT RSS measurement algorithm. Once the

algorithm was executed, it entered into an infinite looping sequence. This looping cycle continued until the network operator terminated the algorithm at the C2 center. Table 3.2 lists and describes the key variables and commands that are shown in Figure 3.10.

Table 3.2: Key variables and commands of SPOT RSS algorithm

Variables	Variable Description	Commands	Command Description
i	loop iteration	i++	add one to previous loop iteration
Count	condition statement for creating clock pulse	CLK.setLow() CLK.setHigh()	applies logic low or high for clock pulse
va1val	measured voltage at A1	va1.get voltage()	retrieves voltage at A1
maximum	maximum voltage value at A1	Pause(3000)	clock pulse duration (msec)
spectrum	loop iteration # where maximum voltage detected	estFreq = floor/ceiling Freq ± increment *spectrum	estimates transmitting frequency
UDcount	applies a logic high or low to U/D pin on U4	UD.setLow() UD.setHigh()	applies logic low or high to U4 U/D pin

The flowchart shows that some variable (i.e., $Count = 1$ and $UDcount = 1$) values and conditions were declared outside the loop sequence. This is important to note because the SPOT will initially clock the PMSA to go up the frequency spectrum due to the termination statement, $i < 129$ to be true and U/D is set high. The clock pulse was created by the variable *count* and the $CLK.set$ command. When *count* alternated between 0 and 1 every three seconds, the clock pulse changed from a high to a low giving it a square pulse appearance.

To increment up the frequency spectrum, the previous loop iteration number after every clock pulse was increased by one ($i++$). At the end of each loop iteration, the voltage measured at the output of the PMSA was compared to a previous

iteration's output voltage value. Once at the top of the spectrum (128 iterations), the termination statement becomes false. The SPOT then sets U4 U/D pin on the PMSA low. The highest voltage recorded at the PMSA output (J3) is converted into a RSS value that is saved to a text file.

The algorithm also recorded the loop iteration number for which the maximum voltage was recorded. This loop iteration number, a variable in the algorithm called *spectrum*, was used to calculate the estimated frequency at which the emitter is transmitting. This was accomplished by knowing the lowest and highest frequency the PMSA was designed to detect. As stated earlier in this chapter, the frequencies which the PMSA can detect depended on the low and high voltage values at the input of pin 3 and pin 6 of U4. These voltage values tuned Y1's output frequency. For example, if pin 3 registered a maximum voltage of 4.90 V during the clock cycle and pin 6 had a minimum voltage of 4.17 V, the PMSA would detect a signal in the frequency range of 2.403 GHz to 2.480 GHz. The difference of the two frequencies was divided by the total number of iterations (128). The resulting number was the amount Y1 incremented or decremented its frequency after each clock pulse. The estimated frequency is illustrated analytically with the following equations

$$increment = \frac{(2.480 - 2.403)GHz}{128\ iterations} \tag{3.2}$$

$$Estimated\ Frequency = 2.403\ GHz + increment \times spectrum \tag{3.3}$$

where on the 60th loop iteration (spectrum) the maximum voltage was detected. This detection corresponds to an estimated frequency of approximately 2.44 GHz. In case the PMSA/SPOT was not able to measure a signal, the estimated frequency was the highest frequency the PMSA could detect. This was true only while going up the frequency spectrum. When the PMSA was clocking down the frequency spectrum and a signal was not detected, the estimated frequency would be the lowest frequency the PMSA can detect. The estimated frequency was also saved in a separate text

file. When the condition of the termination statement $i < 129$ is no longer true, U/D is set low and the looping cycle starts over going down the spectrum due to i being reset to one.

When the network operator has terminated the RSS measurement algorithm, the operator can then import the RSS data text file into the MLE algorithm. The operator also calculates the estimated frequency by finding either the medium or mean of all recorded frequency values saved in the text file. Calculating the medium or mean depends on the number of measurements collected and whether extreme estimated frequency values are recorded.

3.5.3 PMSA/SPOT Quality Control Testing. The purpose of the PMSA/SPOT QC test was to further improve network performance before system calibration and full rate production began. Most of the PMSA design modifications were summarized in Table 3.1, but due to the hardware interface of the PMSA and SPOT, several more modifications were required. During the QC testing of the PMSA test bed, the PMSA was powered by a dual regulated DC power supply. A wireless network would not be mobile if the power supply that had to be plugged into an outlet. This restriction would ultimately lead to performance degradation. The dual DC regulated power supply was replaced by a 12 V 5.0 Amp/Hr rechargeable battery.

A 2.40 GHz to 2.50 GHz, 4 dB omni-directional antenna with a RP-SMA plug connector was used during the PMSA QC test. To increase the distance of the ranging limit of a received signal, a 2.40 GHz to 2.50 GHz, 9 dB omni-directional antenna was used instead. A male connector was added onto the 9 dB antenna to keep the same polarity as J2.

After interfacing the SPOT and PMSA together, the resistance of the voltage divider network R2 and R17 on the PMSA changed. The resistance change led to a less than desired lower voltage at the input of VCO (Y1). Applying Ohm's Law, the SPOT was loading down the PMSA since the input voltage of 6.5 V applied to the voltage divider network did not change. The new voltage at B1 was approximately

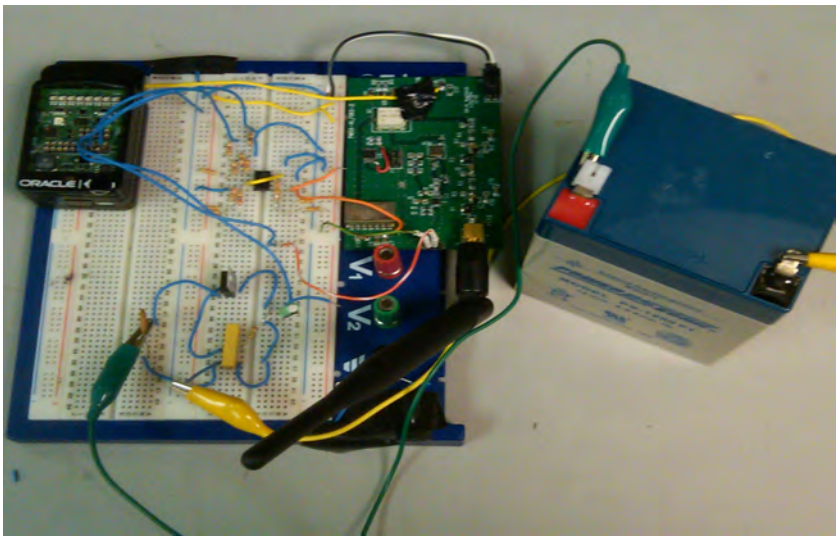

Figure 3.11: SPOT/PMSA prototype.

Table 3.3: Summary of PMSA/SPOT QC testing results

Design Error	Correction	Justification
5 dB rubber duck antenna	Change to 9 dB duck antenna rubber	Increase ranging limit distances
J2 - RP/SMA Jack, female pin	Add male connection pin	9 dB antenna needs to be polarized
R2 and R17 values	R2 = 240 Ω R17 = 240 Ω	SPOT interface decreased U4 pin 6 voltage value
Replaced dual DC regulated power supply	Installed 12 Volt 5.0 Amp/Hr battery	PMSA/SPOT completely wireless and mobile

3.5 V. To increase V_{B1} back to the desired 4.17 V range, R2 and R17 were changed to 220.

Table 3.3 is a summary of the PMSA/SPOT QC test results. Figure 3.11 shows the finished PMSA/SPOT prototype. For the rest of this document, unless otherwise noted, the PMSA/SPOT interface will be referred to as the sensor mote. The overall network performance was analyzed in the calibration phase of the sensor.

3.5.4 Sensor Calibration. Table 3.4 shows an overview of the variables used for the modeling and calibration of the sensor mote described in this subsection.

Table 3.4: Variables used for statistical modeling and calibration of sensor mote

Variable	Definition	Dimensionality or value	Units
RSS	Received Signal Strength	3 x 1	dB
P_0	Transmitted power	3 x 1	dB
RSS_6 RSS_{10} RSS_{14}	Received Signal Strength for $P = 6, 10, 14$ at varying distances in ISM band	9 x 8	dB
$\overline{v}$	Reference voltage	1 x 3	volts
v_s	Averaged measured output voltage of sensor	1 x 9	volts
m	Weighted average of slopes of previous fits	Scalar	dB/volts
$\sigma_{1,2,3}$	Standard deviation of RSS for a given P and distance	depends on # of measurements needed for data fitting	dB
RSS_{ave}	Mean RSS at each measured distance at the given P	Depends on # of measurements needed for data fitting different for every P	dB
d	Measured distances	1 x 8	ft
η	Path loss exponent	1.23	dB/ft
x_0, y_0	Emitter coordinates	Scalar	Unitless
$d(x_0, y_0)$	Path loss component received at each sensor	Scalar	ft

Figures 3.12 and 3.13 show data measurements the sensor and C2 center collected from the signal generator. The voltage peak measurements in the plots represent the average of five data collection runs. The frequency range and the transmitted power to formulate these plots were from 2.403 GHz to 2.48 GHz, incriminated every 8.55 MHz and -6 dB to 14 dB, incriminated every 4 dB. Two notable differences between Figure 3.8 and Figures 3.12 and 3.13 are:

- The (x, y) axes are scaled differently.
- The *least squares* (LS) best fit line is added.

The axes were scaled differently because fewer data points were taken due to the voltage floor being reached at higher transmitted powers and the output voltage peaked at lower values. LS fitting was used because it found the best-fitting line to a

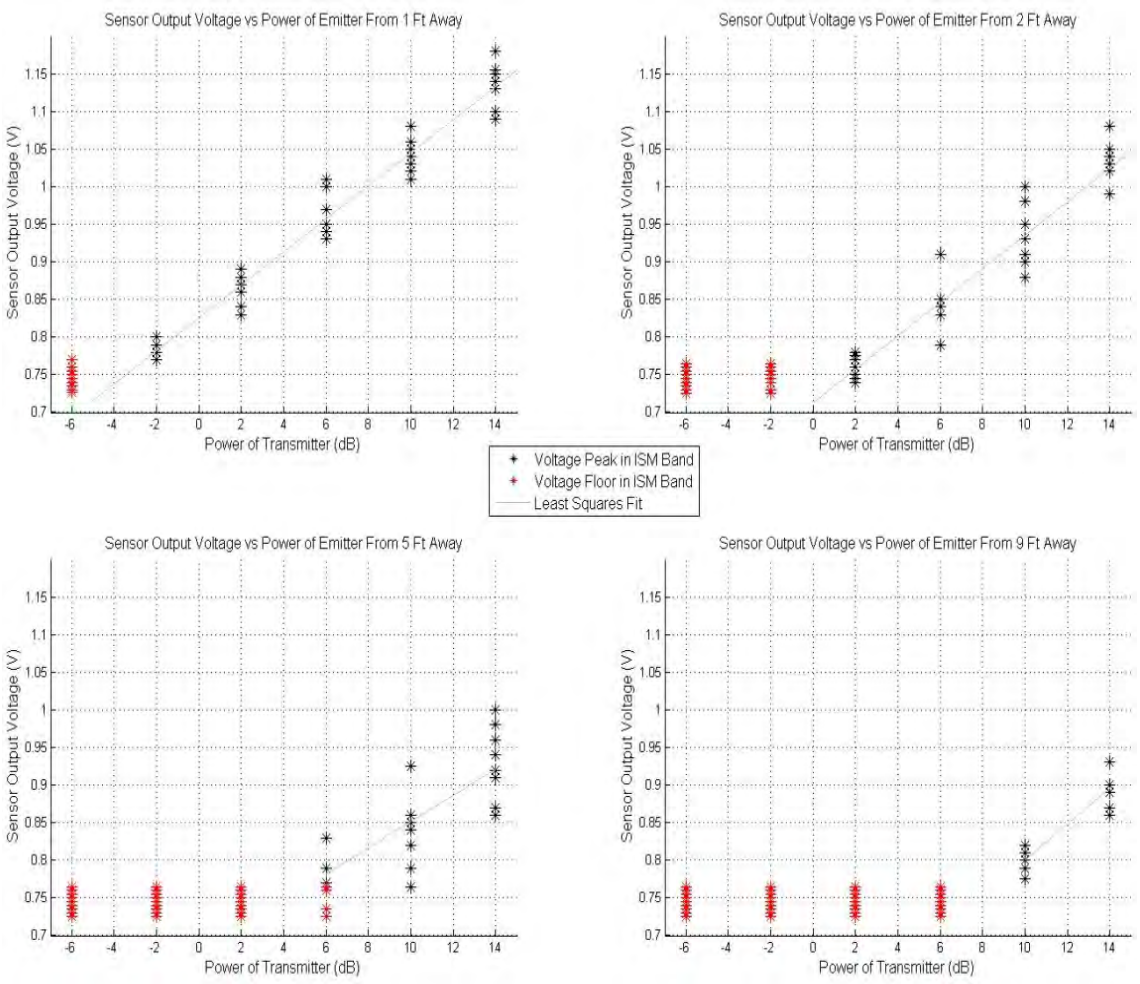

Figure 3.12: Sensor output voltage vs. power of emitter from 1, 2, 5, and 9 ft away.

given set of points by minimizing the sum of squared residuals, a residual being the difference between the observed value and the fitted value. A possible reason behind these changes was the sensitivity of the ADC in the SPOT to read the peak voltages from the PMSA output quickly and efficiently. The slopes ($\boldsymbol{m_d}$) of these best fit lines were used to help create an analytical model that converted voltage per distance ($\boldsymbol{d}$) to RSS per $\boldsymbol{d}$, where $\boldsymbol{d}$ is a vector of the measured distances in feet.

$$\begin{aligned} \boldsymbol{d} &= [d_0, d_1, d_2, d_3, d_4, d_5, d_6, d_7]\ ft \\ &= [1, 2, 5, 9, 10, 11, 12, 13]\ ft \end{aligned} \tag{3.4}$$

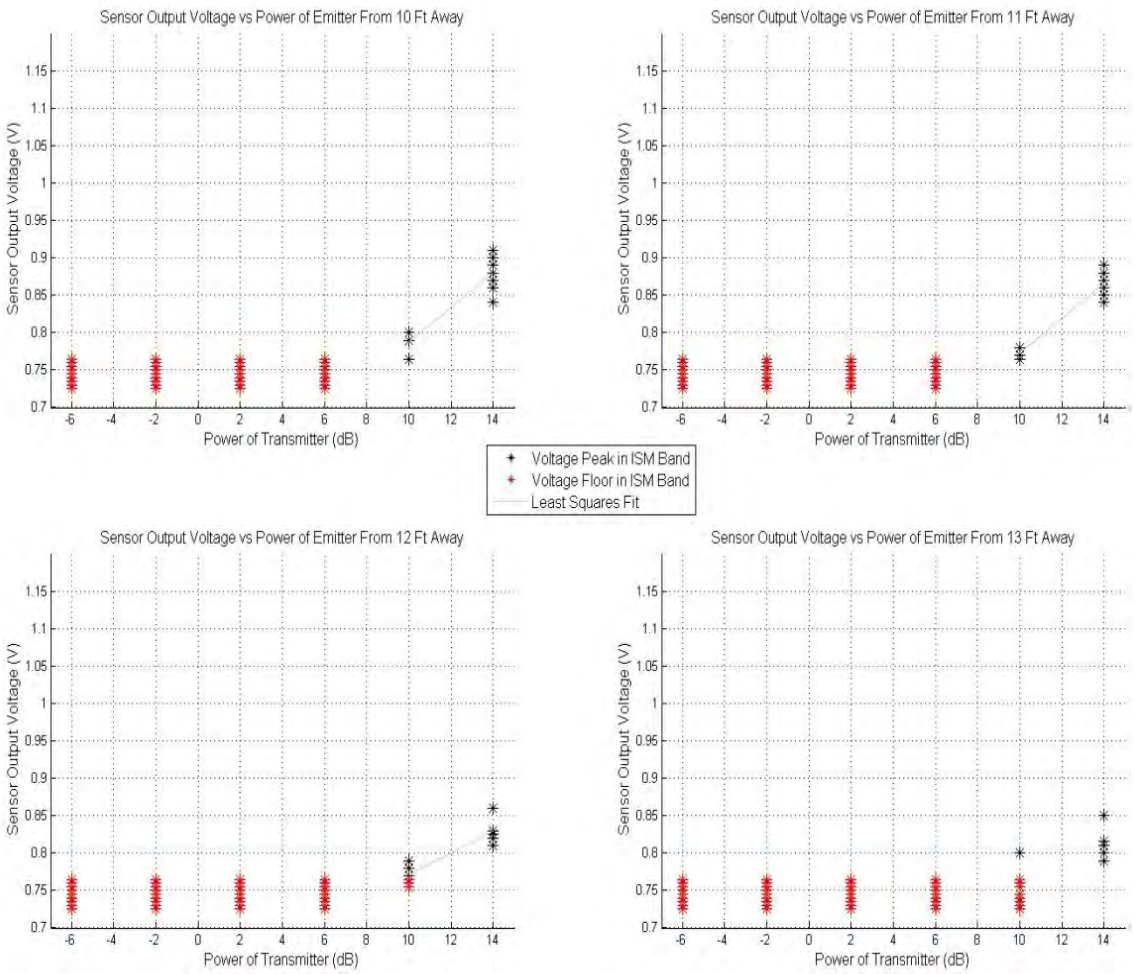

Figure 3.13: Sensor output voltage vs. power of emitter from 10, 11, 12, and 13 ft away.

(3.5) is the weighted average of the slopes of the previous LS lines shown in Figures 3.11 and 3.12.

$$m = \frac{5 \cdot m_{d_0} + 4 \cdot m_{d_1} + 3 \cdot m_{d_2} + 2 \cdot (m_{d_3} + m_{d_4} + m_{d_5} + m_{d_6})}{20} \tag{3.5}$$

where $m = 0.0218 \ \frac{volts}{dB}$. The numbered coefficients in the numerator of (3.5) were based on the number of measurements (excluding voltage floor measurements) taken at each distance. Since the LS fit is a straight line and the weighted average of the slopes, m, has been calculated, the next step was to use the point-slope-intercept straight-line equation of

$$y = -m^{-1} \cdot (x_o - x) + y_0 \tag{3.6}$$

In utilizing (3.6), the measured voltage peak is converted to a RSS value, where

- y is the $\boldsymbol{RSS}$,
- x_0 is the transmitted power $\boldsymbol{P_0}$,
- the weighted slope m is the path loss exponent,
- x_o is the expected voltage peak values $\overline{\boldsymbol{v}}$ at the reference distance d_0, and
- x is the measured voltage peak values $\boldsymbol{v_s}$.

The $\overline{\boldsymbol{v}}$ was calculated by averaging the measured voltage peak values taken in the ISM band for a given transmitted power at d_0. These calculations are shown in (3.7)-(3.10)

$$i = 1, 2..., N \tag{3.7}$$

where $N = 9$, and was the number of data points taken.

$$\overline{\boldsymbol{v}} = \frac{1}{N} \sum_{i=1}^{N} \boldsymbol{v_{si}} \tag{3.8}$$

$$\overline{\boldsymbol{v}} = [0.963,\ 1.039,\ 1.136]^T\ volts \tag{3.9}$$

The three $\overline{\boldsymbol{v}}$ values shown in (3.9) were the expected peak voltage values for the transmitted powers of:

$$\boldsymbol{P_0} = [6,\ 10,\ 14]^T\ dB \tag{3.10}$$

The values in $\boldsymbol{P_0}$ were chosen to ensure the most accurate LS data fit when plotting RSS vs. Distance. As the measured peak voltage values decreased from $\overline{\boldsymbol{v}}$

the lower signal strength was received by the sensor indicating that the sensor was farther away from the emitter. (3.11) is a vector of the measured peak voltage values of size 3×9, where the numbered subscripts in $\boldsymbol{v_s}$ were used to identify the measured peak voltage values for $\boldsymbol{P_0}$.

$$\boldsymbol{v_s} = [\boldsymbol{v_{s_6}},\ \boldsymbol{v_{s_{10}}},\ \boldsymbol{v_{s_{14}}}]^T\ volts \tag{3.11}$$

The vector notation for $\boldsymbol{v_{s_6}}$, $\boldsymbol{v_{s_{10}}}$, $\boldsymbol{v_{s_{14}}}$ indicates the nine measured voltage peak points taken every 8.55 MHz in the ISM band for a given distance. (3.6) can now be written as:

$$\boldsymbol{RSS} = \boldsymbol{P_0} - m^{-1} \cdot (\overline{\boldsymbol{v}} - \boldsymbol{v_s}) \tag{3.12}$$

where $\boldsymbol{RSS}$ is a 3×8 matrix of the received signal strength for $\boldsymbol{d}$. When the transmitted power was $\boldsymbol{P_0}$, $\boldsymbol{RSS}$ simplified to a 3×1 vector. The numbered subscripts in $\boldsymbol{RSS}$ were used to identify the received signal strength for a given transmitted power. Each of the numbered subscripted $\boldsymbol{RSS}$ is a 9×8 matrix. The 9 representing the nine measured $\boldsymbol{v_s}$ data points in the ISM band and 8 indicating the number of distances at which data was collected.

$$\boldsymbol{RSS} = [\boldsymbol{RSS_6},\ \boldsymbol{RSS_{10}},\ \boldsymbol{RSS_{14}}]^T \tag{3.13}$$

Substituting (3.9)-(3.11), (3.13) and the value of m into (3.12) yields

$$\begin{bmatrix} \boldsymbol{RSS_6} \\ \boldsymbol{RSS_{10}} \\ \boldsymbol{RSS_{14}} \end{bmatrix} = \begin{bmatrix} 6 \\ 10 \\ 14 \end{bmatrix} dB - \left(0.0218\frac{volts}{dB}\right)^{-1} \cdot \left(\begin{bmatrix} 0.963 \\ 1.039 \\ 1.136 \end{bmatrix} - \begin{bmatrix} \boldsymbol{v_{s_6}} \\ \boldsymbol{v_{s_{10}}} \\ \boldsymbol{v_{s_{14}}} \end{bmatrix} \right) volts \tag{3.14}$$

Intuitively $\boldsymbol{RSS}$ and $\boldsymbol{P_0}$ will equal each other if $\overline{\boldsymbol{v}}$ and $\boldsymbol{v_s}$ are equal at d_0. As stated previously, the voltage peak measurements in Figures 3.12 and 3.13 represent the average of five data collections measured every 8.55 MHz in the ISM band for a given distance and P_0. This means there were a total of 45 data collections to calculate $\boldsymbol{v_s}$. In substituting $\boldsymbol{RSS}$ from (3.13) into (3.14) the average and standard deviation of the RSS due to the nine $\boldsymbol{v_s}$ for $\boldsymbol{P_0}$ was found.

$$\overline{\boldsymbol{RSS}}_{\boldsymbol{(6,10,14)_{ave}}} = \frac{1}{N}\sum_{i=1}^{N} \boldsymbol{RSS}_{\boldsymbol{(6,10,14)}_i} \tag{3.15}$$

$$\boldsymbol{\sigma_{6,10,14}} = \left(\frac{1}{N}\sum_{i=1}^{N}\left(\boldsymbol{RSS}_{\boldsymbol{(6,10,14)}_i} - \overline{\boldsymbol{RSS}}^{\boldsymbol{2}}_{\boldsymbol{(6,10,14)_{ave}}}\right)\right)^{\frac{1}{2}} \tag{3.16}$$

In Figure 3.14 the $\overline{\boldsymbol{RSS}}_{\boldsymbol{(6,10,14)_{ave}}}$ data points are plotted over $10{\cdot}log_{10}(\boldsymbol{d})$ for the transmitted powers of $\boldsymbol{P_0}$. The error bars in Figure 3.14 correspond to $\boldsymbol{\sigma_{6,10,14}}$. The horizontal dotted blue line represents approximately the lowest transmitted power the sensor mote can detect at d_0 before the measured RSS floor is reached. To tell whether or not the sensor mote received a signal, $\boldsymbol{v_s}$ needed to be above the measured voltage floor. The lowest transmitted power at which the sensor mote detected a signal was -2 dB, which is seen in Figure 3.12 at d_0 . The LS best fit lines are color coded to the $\overline{\boldsymbol{RSS}}_{\boldsymbol{(6,10,14)_{ave}}}$ data points.

Figure 3.14 gives an approximation of the emitters distance from the sensor mote based on the signal strength received at the mote when the transmitted power was $\boldsymbol{P_0}$. To improve the data fit in Figure 3.14, a single LS data line fit was used. To show a single line fit of the RSS measurement points, $\boldsymbol{P_0}$ was defined as 14 dB in (3.14). The substitution, seen in (3.17) shifted the RSS data points for the transmitted powers of 6 and 10 dB up so a better fit was obtained.

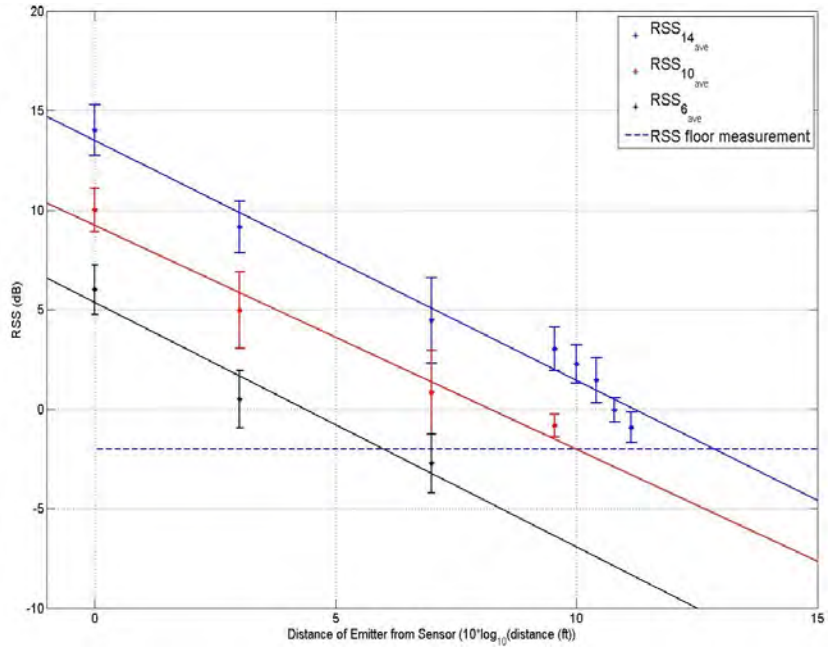

Figure 3.14: The averaged measured RSS vs. Distance for $\boldsymbol{P_0}$.

$$\begin{bmatrix} \boldsymbol{RSS_6} \\ \boldsymbol{RSS_{10}} \\ \boldsymbol{RSS_{14}} \end{bmatrix} = 14\ dB - \left(0.0218\frac{volts}{dB}\right)^{-1} \cdot \left(\begin{bmatrix} 0.963 \\ 1.039 \\ 1.136 \end{bmatrix} - \begin{bmatrix} \boldsymbol{v_{s_6}} \\ \boldsymbol{v_{s_{10}}} \\ \boldsymbol{v_{s_{14}}} \end{bmatrix} \right) volts \quad (3.17)$$

Calculating the average and standard deviation of the $\boldsymbol{RSS}$ values in (3.17) was the same process as it was for (3.14)

$$\overline{\boldsymbol{RSS}}_{\boldsymbol{(6,10,14)_{ave}}} = \frac{1}{N}\sum_{i=1}^{N} \boldsymbol{RSS}_{\boldsymbol{(6,10,14)}_i} \quad (3.18)$$

$$\boldsymbol{\sigma_{6,10,14}} = \left(\frac{1}{N}\sum_{i=1}^{N} \left(\boldsymbol{RSS}_{\boldsymbol{(6,10,14)}_i} - \overline{\boldsymbol{RSS}}^{\boldsymbol{2}}_{\boldsymbol{(6,10,14)_{ave}}} \right) \right)^{\frac{1}{2}} \quad (3.19)$$

Figure 3.15 shows a single LS data fit of the values in (3.18) and the error bars from (3.19).

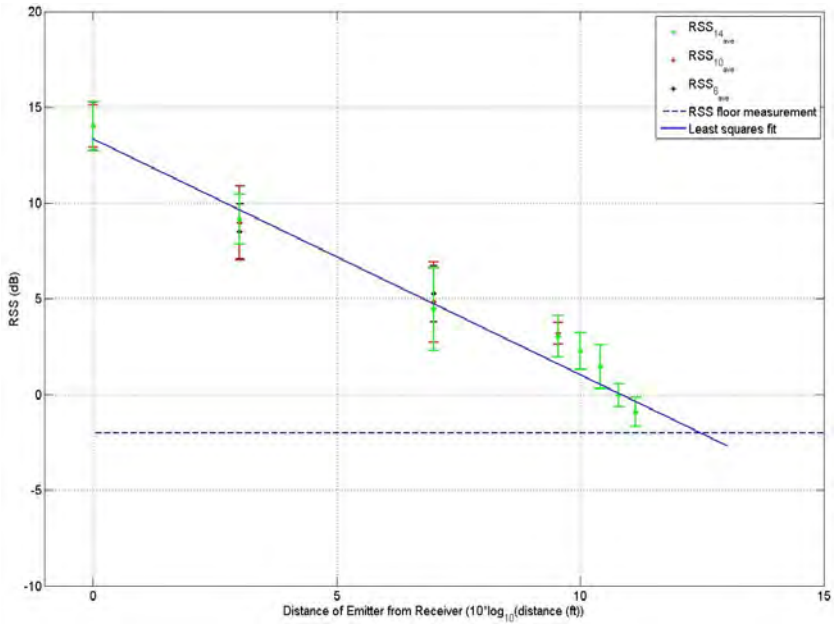

Figure 3.15: The averaged measured RSS vs. Distance for $P_0 = 14$ dB.

$$\boldsymbol{RSS} = P_0 - \eta \cdot 10 \cdot log_{10}(\boldsymbol{d}) \tag{3.20}$$

where $\eta = 1.23\frac{dB}{ft}$ and was the path loss exponent. The path loss exponent was determined by calculating the slope of the LS data fit in Figure 3.15. The service area for this sensor mote was restricted to the RSS ranging limit of approximately 17.5 ft. The ranging limit is where the LS fit intersects with the measured RSS floor. With the exception of different notation and variables, (3.20) closely resembles (2.3).

A Matlab MLE algorithm developed by Dr. Richard Martin, was modified to import the RSS data text file from the Java embedded sensor motes. Under normal conditions (i.e. no measurement floor) a sensor mote should be able to detect signals at greater distances than the sensor mote in this thesis. Normally as the distance increases, there are small traces of the signal received at the sensor that can be distinguishable from noise in the environment. Instead of the RSS reaching a measurement floor as seen in Figures 3.14 and 3.15, the RSS data fit line decreases exponentially as the distance increases, then leveling off before the noise floor is reached. Figure 3.16

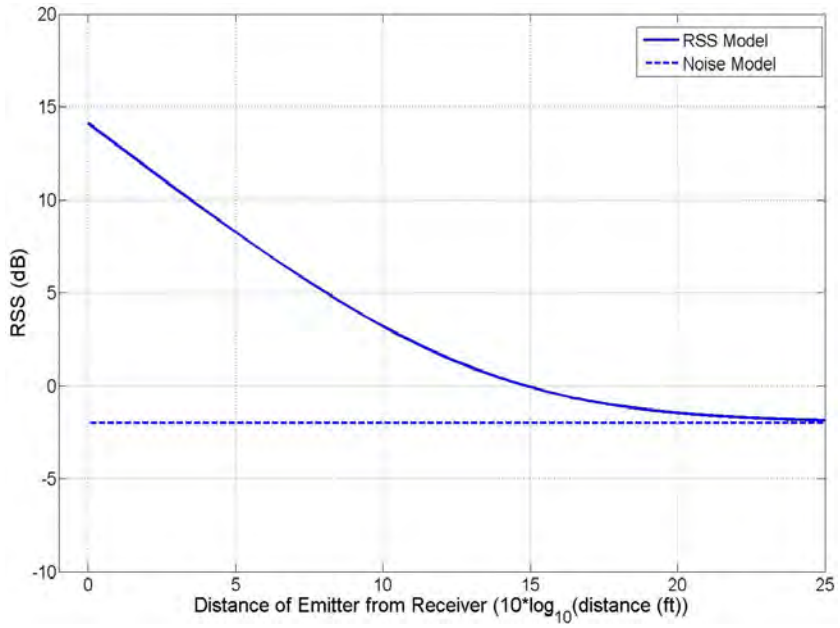

Figure 3.16: RSS data fit under normal conditions.

shows how the RSS data fit would be modeled if the sensor mote in this thesis did not have a measurement floor.

The RSS measurement floor in Figures 3.14 and 3.15 was accounted for in the RSS measurement algorithm. Any time the sensor mote read the voltage floor as the maximum value, the measurement was not converted to RSS. Therefore when a sensor mote measures the voltage floor, the mote does not send a corresponding RSS measurement to the C2 center to be included in the MLE algorithm. The MLE algorithm in Section 2.4.3 was used for estimating a two variable unknown parameter. Since very little is known about a non-cooperative device such as transmitted power, the MLE algorithm was also modified to account for three unknown parameters, P_0 and (x_0, y_0).

3.6 MLE Algorithm Derivation

Table 3.5 shows an overview of the variables used for the modeling estimation of the NN. In this section, an algorithm was derived for estimating the parameters of $\boldsymbol{z} = [x_0, y_0, P_0]$, using only observations of the log-normal distributed received power

Table 3.5: Variables used for statistical modeling and geolocation estimation of NN

Variable	Definition	Dimensionality or value	Units
S	Number of sensors	8	Unitless
x_0, y_0	Emitter coordinates	Scalar	Unitless
z	Unknown parameters	1 x 3	ft and dB
P	Received power vector of all sensors	1 x S	dB
m_s	Average received power at each sensor	Scalar	dB
m	Average received power vector of all sensors	1 x S	dB
σ	Fading channel deviation	6	dB
I	Identity matrix	S x S	Unitless
P_o	Logarithmic transmitted power at d_0	Scalar	dB
η	Path loss exponent	1.23	Unitless
$d_s(x_0, y_0)$	Path loss component received at each sensor	Scalar	ft
w	AWGN	1 x S	dB

at S sensors. Conceptually the process in which this algorithm was derived is similar to the MLE algorithm in Section 2.4 for the cooperative network. The differences in the two algorithms are the variable names and the number of unknown parameters; therefore it would be unnecessary to show the MLE algorithm derivation below in its entirety.

$$\mathbf{P} = [P_1, ..., P_s]^T \sim \mathcal{N}(\boldsymbol{m}, \boldsymbol{C}) \tag{3.21}$$

$$P_s = m_s + w_s \tag{3.22}$$

where $S = 8$ and is the number of sensor motes in network.

$$m_s = P_0 - \eta \cdot 10 \cdot log_{10}(d_s(x_0, y_0)) \tag{3.23}$$

where $\eta = 1.23$ and was calculated in Section 3.5.

For the derivation of the MLE, it is useful to explicitly state the log of the *probability density function* (PDF) associated with (3.21):

$$\begin{aligned} \mathcal{L} &= \ln p(\mathbf{P} \mid \boldsymbol{z}) \\ &= \frac{1}{2}(\boldsymbol{P}-\boldsymbol{m})^T \boldsymbol{C}^{-1}(\boldsymbol{P}-\boldsymbol{m}) \end{aligned} \tag{3.24}$$

The MLE algorithm takes the generic form

$$\hat{\boldsymbol{z}} = arg\ max \underbrace{\ln p(\mathbf{P} \mid \boldsymbol{z})}_{\mathcal{L}}. \tag{3.25}$$

The MLE cost function $\mathcal{L}$ is given by (3.24), and for simplicity $\boldsymbol{C} = \sigma^2 I$. By taking the argument that minimizes $\mathcal{L}$, (3.25) is equivalent to

$$\hat{\boldsymbol{z}} = arg\ min_{\boldsymbol{z}} \|\boldsymbol{P} - \boldsymbol{m}(\boldsymbol{z})\| \tag{3.26}$$

Typically (3.25) is solved by setting its gradient to zero and solving the resulting set of equations. The gradient equations are given by

$$\frac{\partial \mathcal{L}}{\partial z_i} = \sum_{s=1}^{S} (P_s - m_s) \frac{\partial m_s}{\partial z_i} \tag{3.27}$$

where,

$$\frac{\partial m_s}{\partial z_3} = \frac{\partial m_s}{\partial P_0} = 1 \tag{3.28}$$

therefore,

$$\frac{\partial \mathcal{L}}{\partial P_0} = \sum_{s=1}^{S} (P_s - m_s) \tag{3.29}$$

The equations for x_0, y_0 have been omitted since they were highly nonlinear, meaning no closed form solution will exist and a grid search using (3.26) was ultimately necessary in order to solve them.

3.7 Full Rate Production Decision Review

FRPDR is a review normally conducted at the conclusion of the LRIP effort that authorizes entry into *Full Rate Production* (FRP). FRP was defined in this research effort when the sensor networt was produced and deployed to the field to test for *full operational capability* (FOC) [13]. FOC was defined as the ability to geolocate a NN. FRPDR serves as the summary of this chapter and explains why the sensor was ready for FRP.

Compared with other location finding techniques, RSS-based geolocation method has lower location accuracy due to the unpredictable nature of the data measurements. Ideally $\boldsymbol{v_s}$ should decrease as the distance increased. Although this was not labeled in any of the figures, there were a few instances where $\boldsymbol{v_s}$ was higher at a larger distance than a measurement taken at a shorter distance for the same transmitted power and frequency. These higher voltage peak measurements were omitted and a new measurement was taken to consist of the five data collections that were averaged together to plot Figures 3.12 and 3.13.

RSS measurements do have their advantages. RSS measurements are attractive in wireless networks due to their power consumption, size, low complexity and cost. The sensor mote was powered by a rechargeable 12.5 Volt 5.0 Amp/Hr battery. A fully charged battery was able to power the sensor mote for approximately 20 hours before it needed to be recharged, which made the sensor mote's power consumption very low. The sensor mote was transportable, easily fitting in the palm of the hand. The cost per sensor mote was approximately $800. The cost was low but would be considerably lower if the SPOT was specifically designed for this research effort. The cost of a SPOT kit was approximately half of the total cost of the sensor mote.

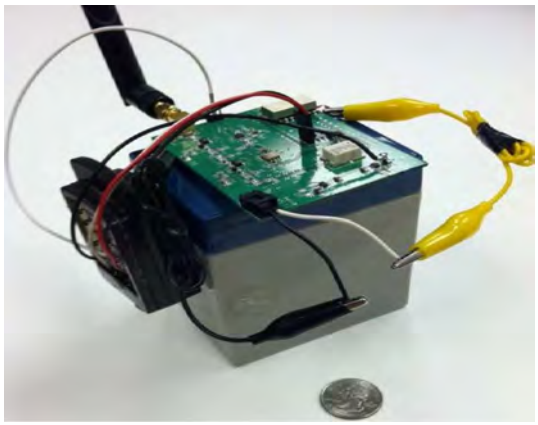

Figure 3.17: Sensor mote: SPOT, PMSA, 12.5 V 5 A/hr rechargeable battery, and 2.40 GHz to 2.50 GHz 9 dB omni-directional antenna.

As stated in Section 1.5 the performance capabilities of the sensor network in this thesis are limited. The SPOT algorithm in Section 3.5.2 does not:

- Aid in geolocating a mobile non-cooperative device.
- Differentiate between multiple non-cooperative devices from a single device. One maximum voltage value is measured.
- Provide a fast clock pulse. The slow clock pulse prevents geolocation a frequency hopping non-cooperative device.

Due to the relative simplistic design and model of the sensor network, limitations were expected. These limitations did not hinder the research objectives. Even with a sensor mote that was limited operationally and practicality, the calibration and modeling results from the LRIP gave the network designer a high degree of confidence that non-cooperative geolocation via RSS can be performed. Therefore, the sensor mote was approved for FRP. Figure 3.17 shows one of the eight manufactured sensor motes deployed to the field to test for FOC.

Chapter IV serves as the basis for FRP as it provides geolocation measurement analysis using different sensor configurations. The sensor network was configured with eight sensor motes that are within a search perimeter of approximately 20×20 ft.

IV. Tests, Results and Analysis

This chapter details the different sensor network configurations that are deployed to the field to test for FOC. The test results are analyzed and discussed in reference to the research objectives. This chapter will include a detailed explanation of the following topics:

1 Geographical layout of sensor network

2 Test results of deployed sensor network to the field

3 Geolocation sources of error via RSS

4 Summary of sensor network's FOC

4.1 Geographical Layout of Sensor Network

Sensor network configurations A and B, seen in Fig. 4.1 are examined in this chapter. The non-cooperative emitter was selectively placed in three different locations by the network designer. The purpose behind varying the locations was to:

- Improve geolocation measurements by ensuring that some of the emitter locations were within the ranging limit of all the sensors.
- Examine the geolocation measurements near and outside the ranging limit of some of the sensors.

When space to set up the sensor network became limited, the distance formula was used to calculate the distance between the sensor and emitter. The sensor motes were then placed accordingly in front of the non-cooperative emitter when testing began.

4.2 Test Results

The test results of the sensor networks in Fig. 4.1 deployed to the field are shown in this section. Two emitting devices were used for testing. These emitters were a

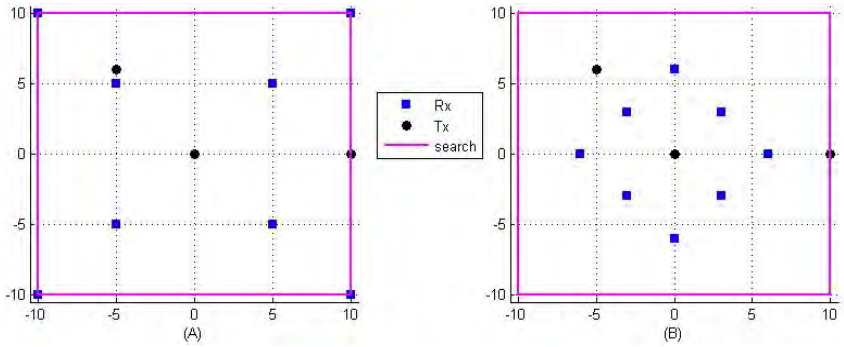

Figure 4.1: Geographical layout of sensor network.

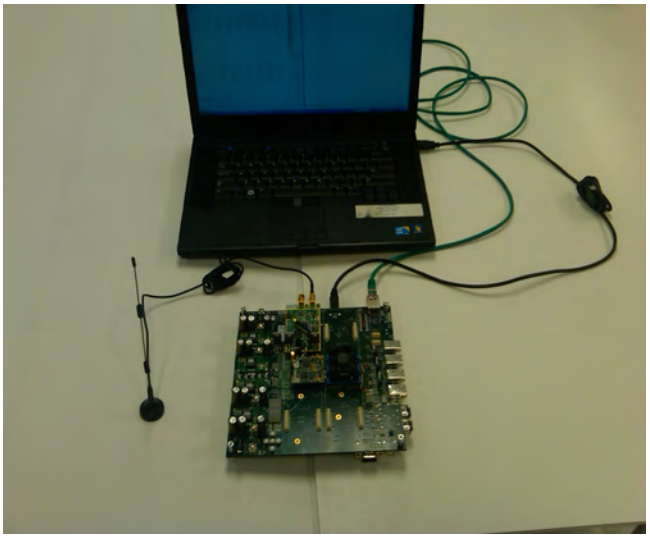

Figure 4.2: Non-cooperative network: WARP, C2 center and antenna [4].

signal generator and a *Wireless Open Access Research Platform* (WARP) device. The WARP device is a scalable and extensible programmable wireless platform used for prototyping advanced wireless networks [4]. The WARP device transmits a random data signal that is modulated by a sine wave. The signal generator used is the same one seen in Fig. 3.7, the WARP is shown in Fig. 4.2. The measured geolocations are shown in the same plots as the simulated geolocation estimates. The goal in comparing the measured and simulated estimates is to show how hardware and environmental-based errors affect geolocation measurements.

The test results plotted in this section are visually similar to the plots in Section 2.4. However, the plots illustrated in Figures 2.5-2.7 were averaged over 100 trials.

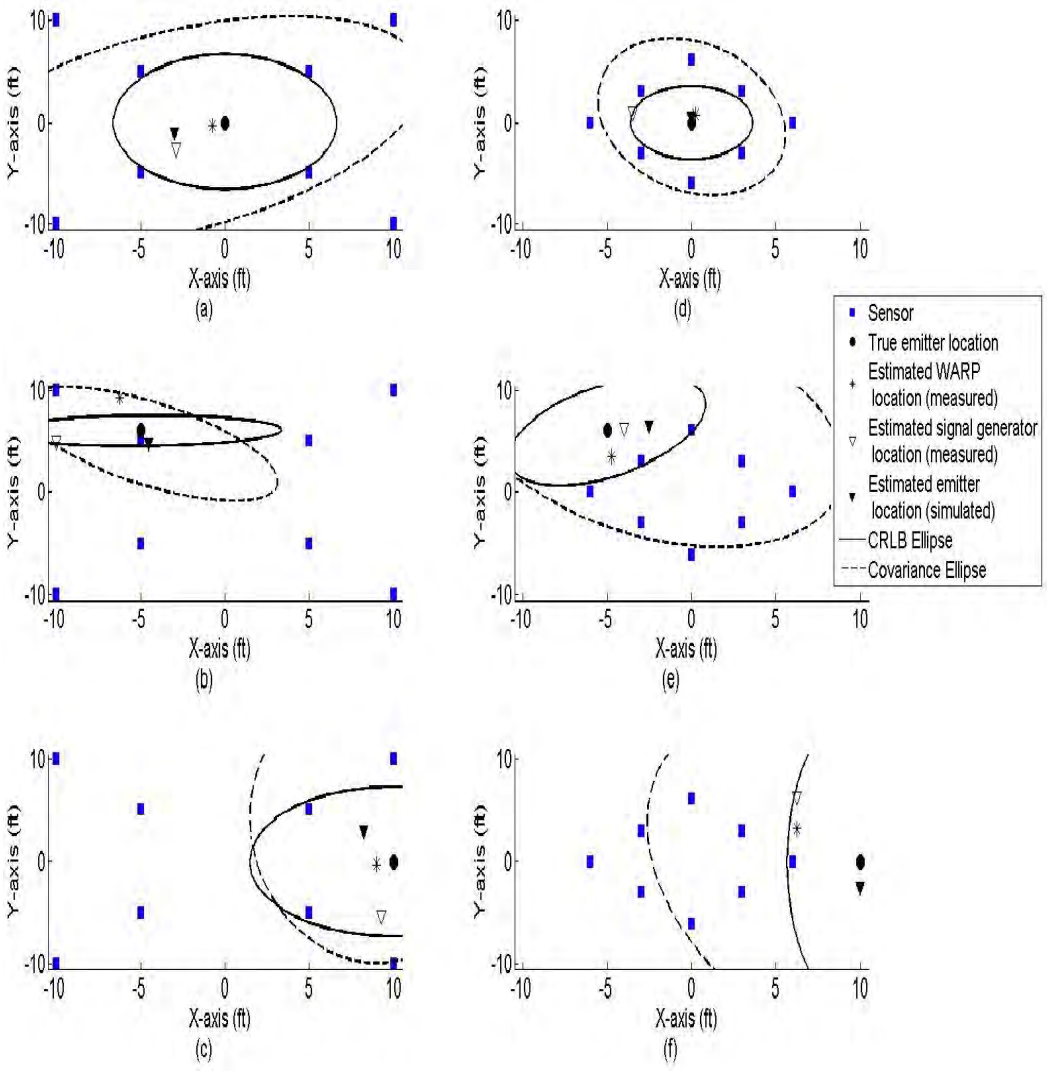

Figure 4.3: Sensor configuration A (a-c) and B (d-f): geolocation estimates of signal generator and WARP device.

Calculating the mean has a disadvantage of being too sensitive to extreme values if the sample size is small. Due to the time it takes the sensor motes to pulse through the ISM band, only 10 measurements were taken at each emitter location for both sensor network configurations. Several of the sensor motes at some point during the 10 measurement collections recorded extreme RSS values. These extreme values are discussed in more detail later in the chapter. The median RSS was less sensitive to extreme measurements and was a better indicator of where the middle value was for the small sample size. To obtain a reasonable comparison between the measured and

Table 4.1: Non-cooperative emitter locations, Root CRLB and RMSE (ft)

Signal Generator (Sig Gen) and WARP Data				
Test	Actual	(0.0, 0.0)	(-5.0, 6.0)	(10.0, 0.0)
A	Simulated Estimate	(-3.00, -1.00)	(-4.50, 4.75)	(8.25, 3.00)
	Sig Gen Measured Estimate	(-2.90, -2.60)	(-10.00, 5.00)	(9.25, -5.25)
	WARP Measured Estimate	(-0.75, -0.25)	(-6.25, 9.25)	(9.00, -0.25)
	Root CRLB	4.37	3.89	5.21
	RMSE	8.68	4.41	6.76
B	Simulated Estimate	(0, 0.50)	(-2.50, 6.50)	(10.00, -2.50)
	Sig Gen Measured Estimate	(-3.50, 1.00)	(-4.00, 6.25)	(6.25, 6.25)
	WARP Measured Estimate	(0.25, 0.75)	(-4.75, 3.5)	(6.25, 3.25)
	Root CRLB	2.39	3.67	7.26
	RMSE	4.42	7.63	10.24

simulated results, the median simulated geolocation estimates were obtained from 10 trials.

Fig. 4.3(a, c-e) shows the measured estimated (signal generator and WARP) geolocations and the simulated geolocations for sensor configurations A and B are within the 90% confidence interval of the CRLB and covariance error ellipses. Fig. 4.3(b) shows the measured estimated WARP geolocation to be inside the covariance ellipse but outside the CRLB ellipse, while the measured estimated signal generator and estimated simulated geolocation are inside both ellipses. Table 4.1 lists the signal generator and WARP locations (actual, simulated and measured) and the simulated data of the Root CRLB and RMSE for sensor configurations A and B.

The estimated frequency for the signal generator was calculated to be 2.425 GHz $\pm$ 12 MHz, while the true transmitted frequency was 2.430 GHz. The estimated frequency for the WARP was calculated to be 2.436 GHz $\pm$ 15 MHz, while the true transmitted frequency had a center frequency of 2.442 GHz and a bandwidth of $\pm$ 6 MHz. The estimated frequencies for both emitters were calculated using (3.3). All estimated frequencies were averaged after each sensor recorded 10 RSS measurements.

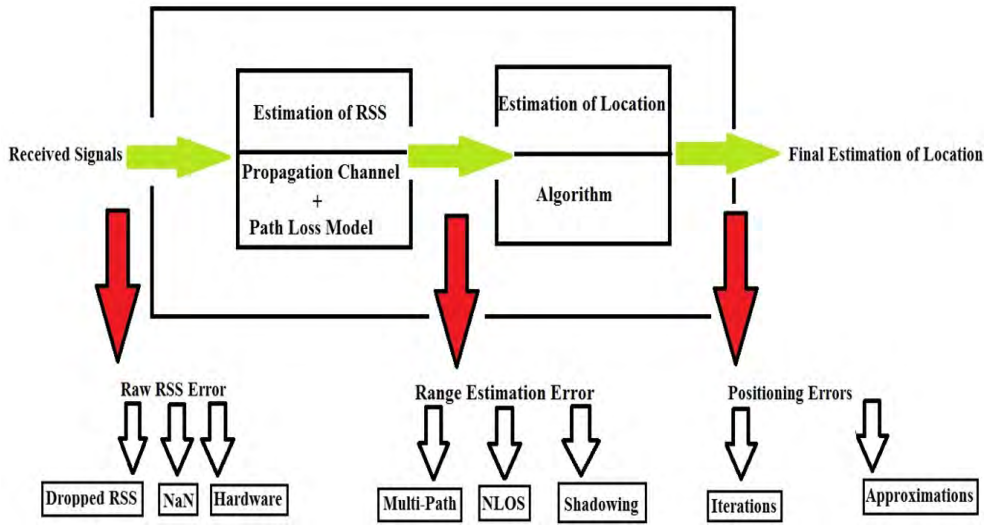

Figure 4.4: Geolocation sources of error via RSS (permission given by author to use figure) [18].

Based on the sensor mote model in Section 3.5, the estimated frequency should vary by approximately 600 KHz from the true transmitted frequency, as this is the desirable size of the frequency increment/decrement the VCO tunes the LO signal after every clock pulse. However, the estimated frequency is within the 12 MHz standard deviation of the true transmitted frequency. The reason the estimated frequency of the signal generator is not within 600 KHz from the true transmitted frequency is discussed in Section 4.3.1. The estimated frequency of the WARP is within 6 MHz of the center frequency.

4.3 Geolocation Sources of Error via RSS

Geolocation sources of error are shown in Fig. 4.4 [18]. The sources of error in geolocation of the simulated CN's in Section 2.5 were caused by:

- AWGN
- The number and positioning of the sensor motes in network
- The number of trials performed in the MLE estimation algorithm

Simulated system models of RSS-based source localization often ignore or estimate hardware and some environment-based errors. Some of these sources of error were briefly discussed in Chapter II. They were NLOS, multi-path, and shadowing. Geolocation sources of error that affected sensor network accuracy are described in this section.

4.3.1 Raw RSS Errors. Hardware limitations of the sensor network have affected the accuracy of the geolocation measurements. As described in Section 3.5, when the sensor mote reads the voltage floor as the maximum value, the measurement is not converted to RSS. The RSS measurement algorithm recorded the measurement as a zero. If a sensor recorded a zero for all 10 measurement collections, it was assumed that the sensor was outside the ranging limit of the transmitter. If the sensor was outside the ranging limit, the data collected from that sensor were not used to calculate the measured geolocation of the NN. A RSS value of zero in all measurement collections by a sensor mote is referred to as a *Dropped RSS*. Generally as the number of sensors in the network collecting usable data decreases, the accuracy of the geolocation measurement will also decrease.

Although the sensor mote prototype model was built to measure RF signals transmitting approximately between 2.403 GHz to 2.48 GHz, all sensors operating in the network have a different frequency range. Some sensor motes received signals outside the ISM band resulting in the frequency range difference to be greater than 77 MHz. This caused the sensor to record the maximum voltage as the measurement floor due the size of LO signal's frequency increment or decrement to be greater than 600 KHz after each clock pulse. Ideally LO frequency changes should be less than or equal to 600 KHz so that at least one of the 128 VR settings will have the IF frequency to be between 314.7 MHz and 315.3 MHz so that the filter can pass the signal to the power detector. In the case that the RSS value was equal to zero during some of the measurement collections the value was referred to as a *Not a Number* (NaN), because the sensor mote's frequency range was greater than 77 MHz. Further

system modeling and calibration are needed to better identify NaNs from RSS values that are equal to zero. Due to the 12 MHz bandwidth of the WARP device and the 600 KHz increment at the end of each clock pulse, NaNs were not present when the sensor network was measuring the RSS of the WARP device. The sensor network measured several voltage peaks when the WARP was transmitting. The ability of the sensor network to receive signals outside the ISM band caused the difference between the estimated frequency and true transmitted frequency of the signal generator to be greater than 600 KHz.

The hardware was limited in how fast it could measure voltage after each clock pulse. This limitation was due to the slow sampling rate of the ADC of the SPOT's A1 port. If the clock pulse was set too fast, the sensor will display an extreme RSS value. As shown in Fig. 3.10, the clock pulse was set to three seconds, which is slow and not practical for performing real-time measurements.

The FRP of the sensor motes was based on the sensor mote prototype model and calibration results described in Section 3.5. According to Fig. 3.15, when the sensor motes were located at the reference distance of one feet (d_0) from an emitter transmitting at 14 dB, the motes should measure a RSS value between 12.75 - 15.25 dB. The error bars in Fig. 3.15 show the measured RSS can vary by a few feet from the expected RSS. The error bars were calculated from averaging five voltage peak collections, measured at nine different frequencies while the transmitted power was adjusted from 14, 10 and 6 dB, for a total of 135 RSS measurements. Fig. 4.5 shows the mean (μ) and standard deviation (σ_{std}) of 10 RSS measurements at d_0 for the sensor motes operating in the network. Only five out of the eight sensor motes in the network were within the expected RSS measurement range as seen in Fig. 3.15.

There are electrical parameters and characteristics of the eight sensor motes used to test for FOC that vary from the sensor mote prototype that was modeled and calibrated in Chapter III. Several of the sensor motes had an expected RSS greater than 14 dB at d_0. These larger than expected RSS measurements indicate that $\boldsymbol{v_s}$ in

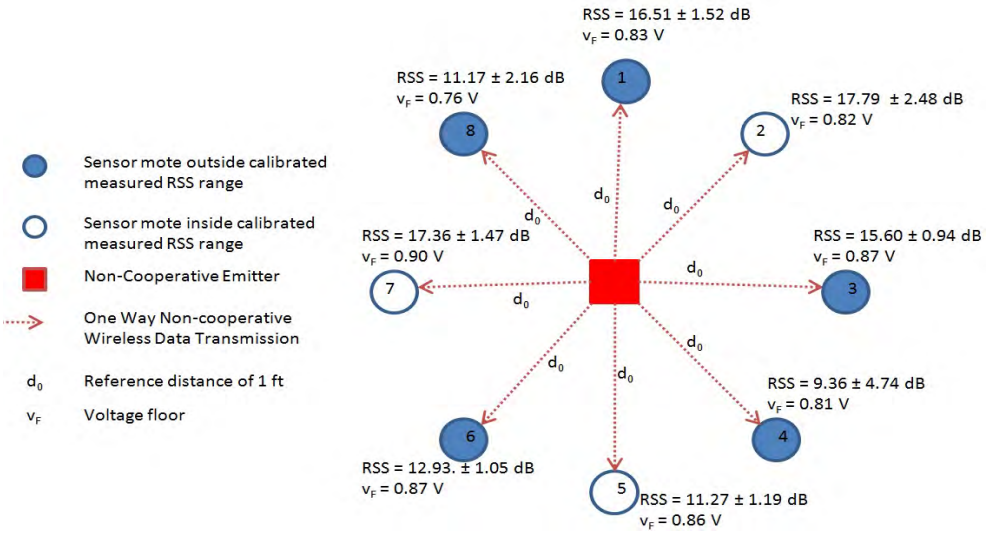

Figure 4.5: Raw RSS error caused from hardware: The μ and σ_{std} of 10 RSS measurements at $d_0 = 1$ ft and voltage floor for each sensor mote operating in the network.

(3.12) was greater than $\overline{\boldsymbol{v}}$. Also seen in Fig. 4.5 is the voltage floor for every sensor mote used in the network. The voltage floor for the prototype model measured 0.65 V to 0.76 V. The measurement floor cutoff of 0.76 V was then programmed into the RSS measurement algorithm. Since seven of the eight sensor motes used for testing have a higher voltage floor than the measurement floor cutoff of 0.76 V, RSS vs. Distance resembled the model shown in Fig. 3.16 instead of the intended model in Fig. 3.15. It was difficult to determine how much the ranging limit, RSS measurement floor and the path loss exponent have changed from the calibration results in Chapter III due to the variations in the voltage floor and the expected RSS measurements. These changes in the voltage floor and expected RSS measurements and their impact on the ranging limit, RSS measurement floor and the path loss exponent are discussed further in Section 5.4.

4.3.2 Range Estimation Errors. In real-world channels, multipath and shadowing are two major sources of environment dependencies affecting the measured RSS. The sensor motes operating in the network experienced shadowing, due to the attenuation of the transmitted signal from obstructions. These obstructions such as

furniture, walls and buildings are common since it is not practical to deploy a sensor network into an open field to geolocate a hostile emitter.

4.3.3 Positioning Errors. In Section 2.4, the RSS is subtracted from the transmitted power and then assumed that the error (the difference) is characterized by a Gaussian distribution. The MLE was then averaged over 100 trials. In this chapter, the measured and simulated geolocation estimates could have obtained better accuracy if more trials were run and measurements were collected. This may have allowed the mean MLE to be calculated instead of calculating the median RSS from 10 measurements which resulted in a single MLE.

4.4 Summary of Sensor Network's FOC

Testing the sensor network for FOC showed how processing raw RSS and hardware limitations can introduce error into the geolocation estimate. Processing raw RSS and hardware limitations are generally not accounted for when calculating simulated estimates. Strict conditions were used to identify voltage floor cutoffs, *Dropped RSS*, and $NaNs$. Signal detection theory, the ability to discern between information-bearing signal patterns and noise, was not conducted during this research effort. Applying signal detection theory to this research effort is a topic discussed in Chapter V under the future work section. The performance of the sensor network was excellent, as both non-cooperative emitters used to test for FOC are within the CRLB and/or covariance error ellipses. Even though each sensor mote will have to be individually recalibrated, accurate geolocation results were obtained. A median RSS value from 10 Raw RSS measurements was used to obtain one MLE measurement. By obtaining one MLE measurement it was difficult to make a fair comparison with an averaged MLE simulated estimate calculated from 10 trials. However, once recalibration is completed, an MLE measured estimate can be calculated for each data collection and then averaged.

V. Summary, Conclusions and Future Work

This chapter discusses the summary, conclusion, contributions, and future research possibilities in this area of study. Current research discussed in Chapter II along with work involved with the research outlined in Chapter III and IV will be the basis for possible follow-on research efforts.

5.1 Summary

The work began by providing a statistical analysis and estimation of a simulated CN RSS system in Section 2.4. Understanding how a CN RSS system operated was useful in characterizing and testing a NN in Chapters III and IV. The research then shifted to learn how the PMSA was designed to operate. During PMSA QC testing, the PMSA (ver.1) was found to be inoperable. Once the design errors were fixed and the appropriate modifications were made, the PMSA was ready for IOT&E. The results of the IOT&E verified and validated the successful redesign of the PMSA (ver.2) and proper set up of the test bed to further develop a working sensor mote prototype. By the conclusion of LRIP the

- PMSA and SPOT were interfaced through the use of hardware and software,
- the PMSA and SPOT RSS measurement algorithm was developed,
- further QC testing was done to improve network performance due to the PMSA and SPOT interface, and
- the sensor mote had been calibrated, modeled and tested over some protracted amount of time.

Before authorizing entry into the FRP and deployment effort, a FRPDR was conducted. Due to the calibration, modeling and test results from the LRIP, the FRPDR concluded with a high degree of confidence that non-cooperative geolocation via RSS could be performed. Before eight sensor motes were deployed to the field to test for FOC, (1) a derivation of a MLE algorithm developed at AFIT was shown, and (2) a geographical layout of two sensor network configurations was created.

The research concluded by comparing the measured geolocation of two non-cooperative networks to the simulated estimate. This comparison showed how hardware and environmental effects have introduced error into the geolocation measurements.

5.2 Conclusion

Cooperative localization networks and measurement techniques are a well understood topic. This research effort developed a low cost, low complexity, small, and energy efficient sensor network to measure geolocation of a NN via RSS. In doing so, this research effort has successfully accomplished all the research objectives as outlined in Section 1.4.

The functionality of the PMSA and SPOT interface does allow for the detection and geolocation via RSS of wireless signals over the ISM frequency band. The detection and geolocation of the sensor motes were achieved by modifying an existing algorithm that measured RSS from a NN. This thesis also investigated how hardware and environmental effects have introduced error into the network by comparing measured non-cooperative geolocation data to simulated estimates. The results from the geolocation tests that were conducted and described in Section 4.3 verify and validate the successful FOC of the sensor network designed in this research effort by obtaining accurate measured geolocation estimates. All the measured geolocation estimates of the signal generator and WARP device for both sensor network configurations were within the 90% confidence intervals of the CRLB and/or covariance error ellipses. This research effort also included developing an algorithm to estimate a non-cooperative emitter's transmitted frequency to within 15 MHz of the true transmitted frequency.

5.3 Contributions

As a result of this research effort, a two page poster abstract titled, "Low Cost Sensor Design For Non-Cooperative Geolocation Via RSS" was written and presented at the 9^{th} *European Conference on Wireless Sensor Networks* held at the Uni-

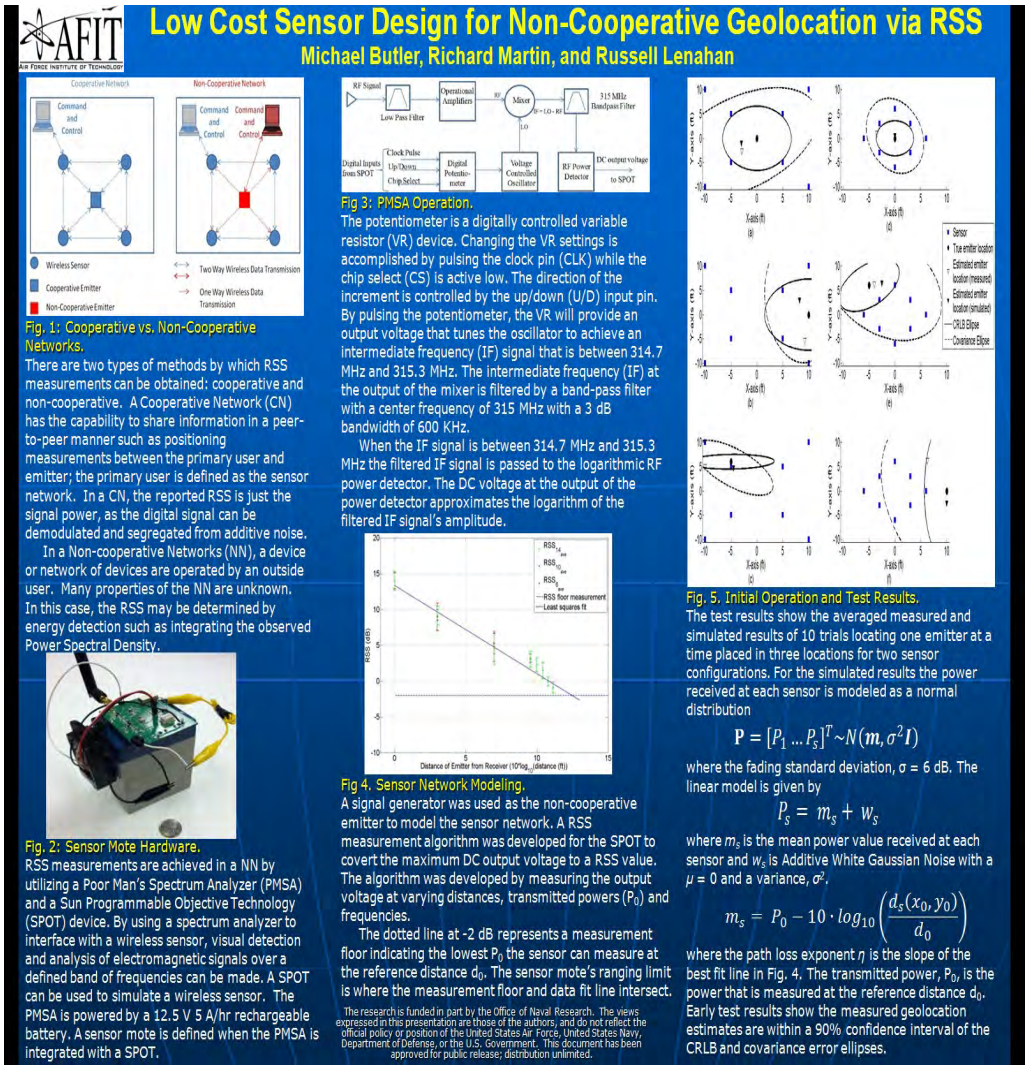

Figure 5.1: Poster presented at 9^{th} *European Conference on Wireless Sensor Networks*.

versity of Trento, Italy, on February 15-17, 2012. This conference was the ninth of a series of annual meetings focused on the latest research in the area of wireless networks. The poster abstract is attached to the Appendix of this thesis paper and the poster is shown in Fig. 5.1.

A patent on the PMSA is currently being pursued. The co-inventors, Captain Michael Butler and Dr. Chris Anderson of the United States Naval Academy, began the patent application process by completing a *Disclosure* and *Record of Invention* form AF1279 and AFRL/RYR is completing the *Evaluator* form AF1981.

5.4 Future Work

There are areas within this subject matter that justify future research. The topics for future work correspond to improving the current design and operational capability of the sensor network. These topics are:

- Hardware design
- Network modeling and calibration
- Network limitations

5.4.1 Hardware Design. The SPOT is an embedded microprocessor device, programmed to interface with the PMSA for this research effort. Follow-on work could look into designing future versions of the PMSA with a Java embedded integrated circuit that provides the inputs to the CLK, CS and U/D pin of the digital potentiometer. The benefit of this design change is it would:

- Simplify wiring
- Simplify RSS measurement algorithm implementation
- Lower energy consumption

An external power source (i.e., 12 V 5A/hr rechargeable battery) would then not be needed to drive the high current/voltage I/O H0-H3 pins. The PMSA would be powered by the SPOT. This would be accomplished by connecting the 3 V and 5 V pin on the demo sensor board in series to obtain a higher voltage, as at least 6.5 V is needed to turn on the PMSA.

The soldering of the wires connecting the SPOT to the PMSA created quality control issues. On several occasions wiring came loose and electrical connection was lost. Only one wire (A1 to J3) would be needed to measure the DC output voltage of the RF Power Detector and send the calibrated RSS value to the base station. These changes would lead to a smaller, lower cost, lower complexity and more energy efficient sensor design.

5.4.2 Network Modeling and Calibration. Figure 4.5 revealed the measured RSS at d_0 and measurement floor of every sensor mote are different and in some cases these differences are extreme (i.e., 8 dB between sensors 2 and 4 and 0.14 V between sensors 7 and 8). These differences in the voltage floor and expected RSS measurements will impact the ranging limit, RSS measurement floor and the path loss exponent. In order to ensure the sensor network can achieve the most accurate measured geolocation estimate, every sensor mote needs to be individually calibrated and then programmed with a separate RSS measurement, estimated frequency, and cut-off voltage algorithm.

Future research could also consist of signal detection theory. Detection theory can aid in identifying and differentiate between *Dropped RSS* and NaN measurements. By programming a cut-off voltage into the sensor network, a sensor mote may not be able to measure a signal near the ranging limit due to the small gain in the voltage floor as frequency increases. Instead of calling all 0 RSS measurement values that appear sporadically throughout the data set a NaN, detection theory will help to identify if the IF signal was outside the desired 315 MHz $\pm$ 600 KHz throughout the entire frequency spectrum sweep.

5.4.3 Network Limitations. Once the sensor network is recalibrated and tested, the network can be programmed to geolocate multiple non-cooperative devices by converting multiple voltage peaks into RSS. The time or the estimated frequency in which an RSS measurement was taken could be used as the starting point to distinguish how many and where the emitters are located.

Appendix A. PMSA Schematics and Poster Abstract

Figures. A.1 and A.2 in this Appendix show the electrical schematic of the original (ver.1) and redesigned PMSA (ver.2). Ver. 2 does not show voltage regulators U5 and U6, as these components did not change between versions.

This Appendix also includes the two page poster abstract presented at the 9^{th} *European Conference on Wireless Sensor Networks* held at the University of Trento, Italy, on February 15-17, 2012.

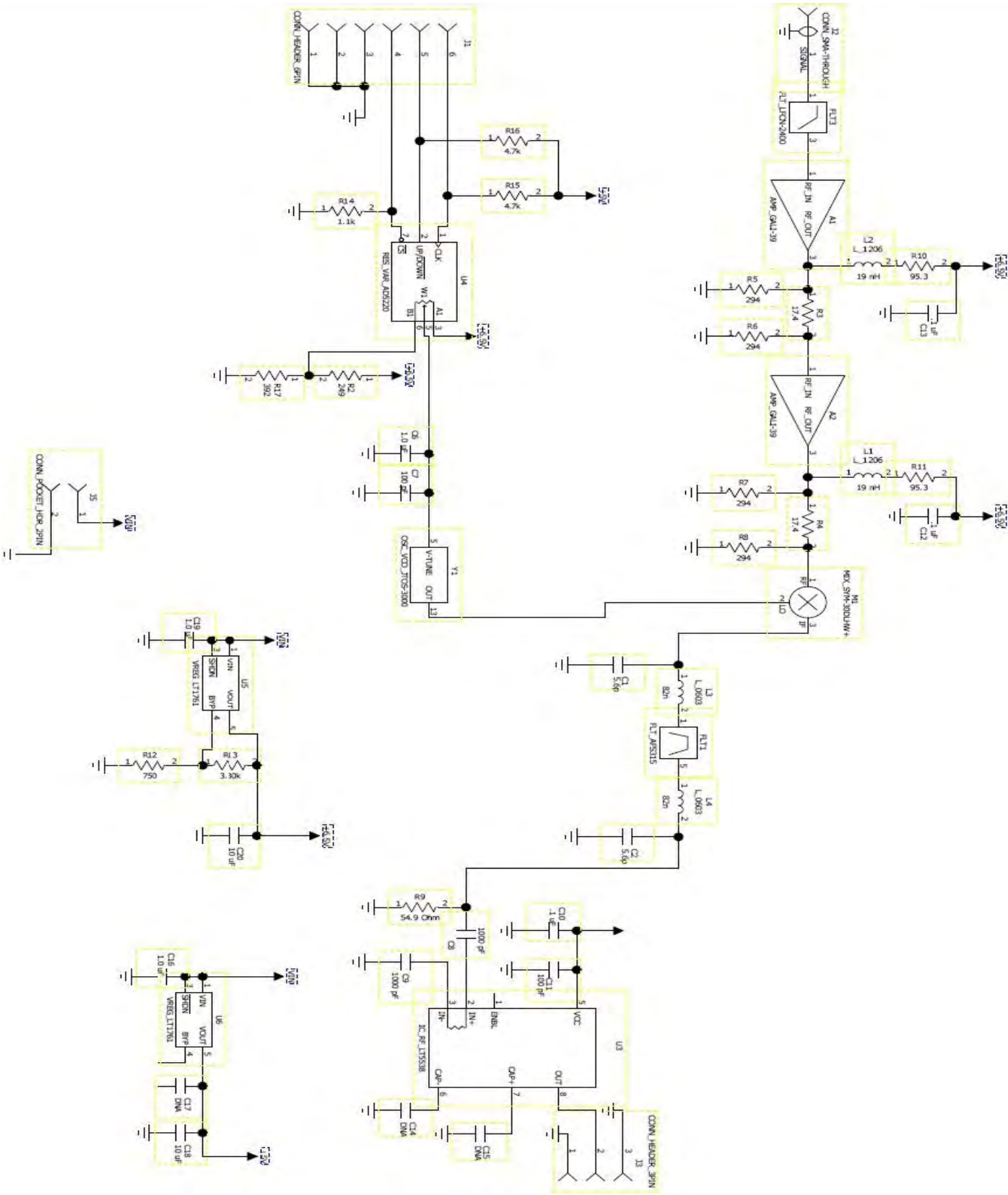

Figure A.1: PMSA ver.1 Schematic

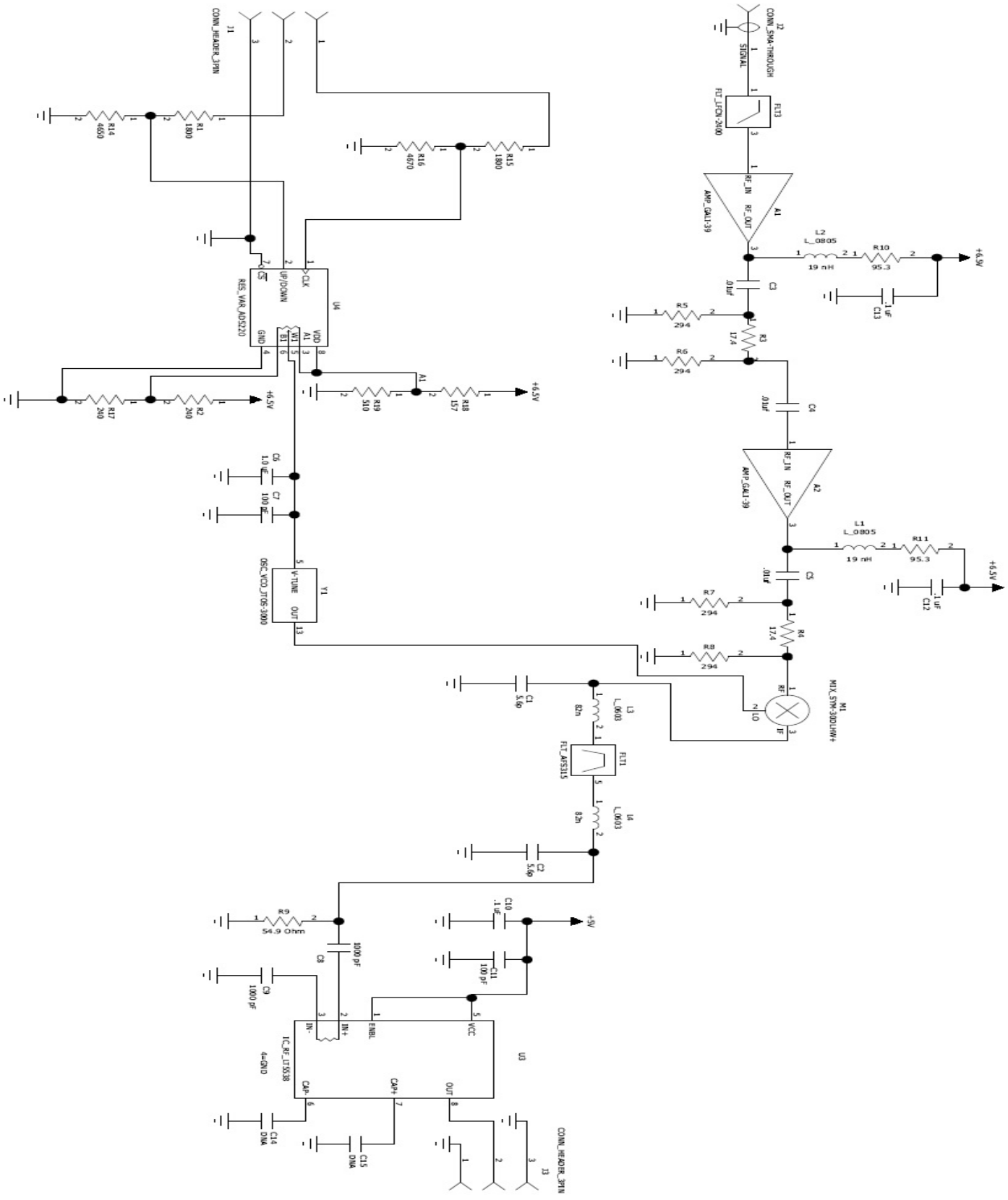

Figure A.2: PMSA ver.2 Schematic

Poster Abstract: Low Cost Sensor Design for Non-Cooperative Geolocation via RSS

Michael S. Butler, Richard K. Martin, and Russell Lenahan
The Air Force Institute of Technology Dept. of Elec. & Comp. Eng.

***Abstract*— Obtaining accurate non-cooperative geolocation is vital for persistent surveillance of a hostile emitter. Current research for developing a small, cheap and energy efficient sensor network for non-cooperative geolocation measurements via received signal strength (RSS) is thin. Most existing work focuses on simulating a non-cooperative network (NN) and in doing so, simulated models often ignore localization errors caused from the hardware processing raw RSS data and often model environment-dependent errors as random. By comparing real-time measured non-cooperative geolocation data to a simulated system a more accurate model can be developed. In this poster we discuss the development of a sensor network that can locate a NN via RSS.**

I. Introduction

Geolocation is the process of using a wireless sensor network (WSN) to locate and track the position of a radio emitter. Four common measurement methods can be used for localization of wireless devices. They are RSS, AOA, TOA, and TDOA. For comparison, AOA requires more complex hardware on each sensor (such as an antenna array). TOA requires cooperation between the emitter and sensors for precise timing. TDOA uses relative time measurements at each receiving sensor in place of absolute time measurements [1], [2]. Though each measurement type has its own merits, this paper focuses on RSS.

There are two types of methods by which RSS measurements can be obtained: cooperative and non-cooperative. In a cooperative network, the device to be located may share parameter values with the WSN. In such cases, the reported RSS is just the signal power, as the signal can be demodulated and segregated from additive noise [1], [3].

In NNs, many properties of the emitter are unknown. The RSS may be determined by energy detection such as integrating the observed Power Spectral Density (PSD) [1], [3]. Fig. 1 shows the differences between a CN and NN.

II. Non-Cooperative System Architecture

RSS measurements are achieved in a NN by utilizing a Poor Man's Spectrum Analyzer (PMSA) and a Sun Programmable Objective Technology (SPOT) device. By using a spectrum analyzer to interface with a wireless sensor, visual detection and analysis of electromagnetic signals over a defined band of frequencies can be made. A SPOT can be used to simulate transducers and WSN motes. A majority of the research effort had been focused on successfully designing the PMSA. A sensor mote is defined when the PMSA is integrated with a SPOT.

This work is funded in part by the Office of Naval Research. The views expressed in this paper are those of the authors, and do not reflect the official policy or position of the United States Air Force, Navy, Department of Defense, or the U.S. Government. This document has been approved for public release; distribution unlimited.

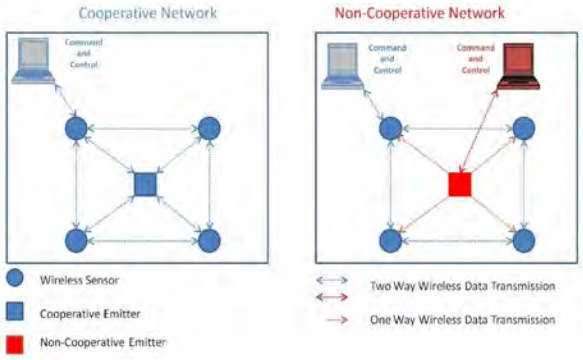

Fig. 1. Cooperative vs. Non-Cooperative Network

Another component of the RSS system architecture is a non-cooperative emitter transmitting in the ISM band. The controlling operations and algorithm implementations of the sensor motes are performed in the Command and Control (C2) center. The C2 center consists of a SPOT base station and laptop computer. The base station unit communicates wirelessly with the SPOT, which then streams the data via a USB connection to the host computer.

III. PMSA Theory Of Operation

As shown in Fig. 2, the potentiometer is a digitally controlled variable resistor (VR) device. Changing the VR settings is accomplished by pulsing the clock pin (CLK) while the chip select (CS) is active low. The direction of the increment is controlled by the up/down (U/D) input pin. By pulsing the potentiometer, the VR will provide an output voltage that tunes the oscillator to achieve an intermediate

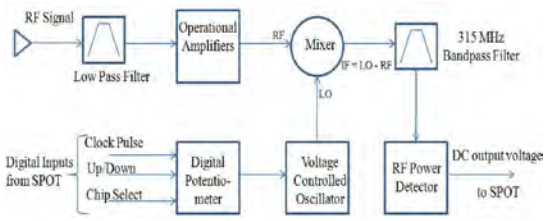

Fig. 2. PMSA Block Diagram

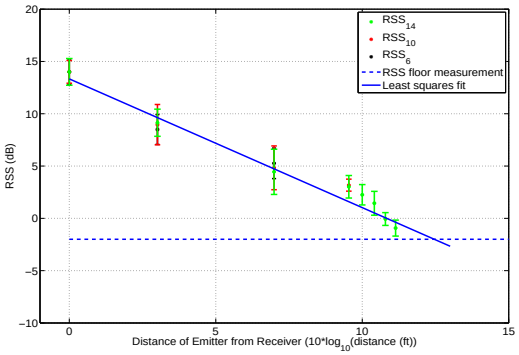

Fig. 3. RSS vs. Distance

frequency (IF) signal that is between 314.7 MHz and 315.3 MHz. The intermediate frequency (IF) signal at the output of the mixer is filtered by a band-pass filter with a center frequency of 315 MHz with a 3 dB bandwidth of 600 KHz.

When the frequency of the IF signal is between 314.7 MHz and 315.3 MHz the filtered IF signal is passed to the logarithmic RF power detector. The DC voltage at the output of the power detector approximates the logarithm of the filtered IF signal's amplitude. The SPOT is programmed to provide the inputs to the CLK, CS pin, U/D input pin and measure the DC output voltage.

IV. Sensor Network Modeling

A signal generator was used as the non-cooperative emitter to model the sensor network. A RSS measurement algorithm was developed for the SPOT to covert the maximum DC output voltage to a RSS value. The algorithm was developed by measuring the output voltage at varying distances, transmitted powers (P_0) and frequencies.

Fig. 3 is a plot of the RSS at each distance a measurement was taken for P_0 = 6, 10 and, 14 dB. The RSS data points for P_0 = 6 and 10 were shifted up to obtain a better line fit. The dotted line at -2 dB represents a measurement floor indicating the lowest P_0 the sensor can measure at the reference distance d_0. The sensor mote's ranging limit is where the measurement floor and data fit line intersect.

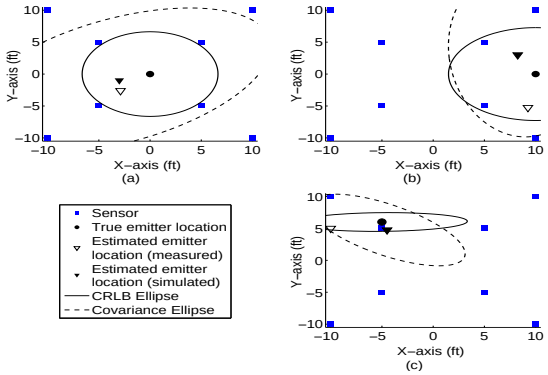

Fig. 4. Measured vs. Simulated geolocation

V. Initial Operation and Test Results

Fig. 4 shows the averaged measured and simulated results of 10 trials locating one emitter at a time placed in three locations. For the simulated results the power received at each sensor is modeled as a normal distribution

$$\mathbf{P} = [P_1, ..., P_s]^T \sim N(\boldsymbol{m}, \sigma^2 \boldsymbol{I}) \quad (1)$$

where the fading standard deviation, σ = 6 dB. The linear model is given by

$$P_s = m_s + w_s \quad (2)$$

where m_s is the mean power value received at each sensor and w_s is Additive White Gaussian Noise.

$$m_s = P_0 - \eta \cdot 10 \cdot \log_{10}\left(\frac{d_s(x_0, y_0)}{d_0}\right) \quad (3)$$

where the path loss exponent η is the slope of the best fit line in Fig. 3. Test results show the measured estimates are within a 90% confidence interval of the Cramer-Rao Lower Bound (CRLB) and covariance error ellipses.

VI. Conclusion

This poster has presented a small, low cost and energy efficient sensor network to measure non-cooperative geolocation via RSS. The successful design of the sensor network was supported by presenting measured geolocation estimates. Future work will consist of improving sensor network modeling and collecting RSS measurements on practical non-cooperative devices.

References

[1] N. Patwari, J. N. Ash, S. Kyperountas, A. O. Hero, III, R. L. Moses, and N. S. Correal, "Locating the nodes: cooperative localization in wireless sensor networks", *IEEE Signal Processing Mag.*, vol. 22, no. 4, pp. 54-69, July 2005.

[2] G. Mao, B. Fidan, and B. D. O. Anderson, "Wireless sensor network localization techniques", *Comput. Netw.*, vol. 51, no. 10, pp. 2529-2553, Jan. 2007.

[3] H. Wymeersch, J. Lien, and M. Z. Win, "Cooperative localization in wireless networks", *Proc. IEEE*, vol. 97, no. 2, pp. 427-450, Feb. 2009.

Bibliography

1. "40 MHz to 3.8 GHz Radio Frequency Power Detector with 75 dB Dynamic Range". URL `http://cds.linear.com/docs/Datasheet/5538f.pdf`. Accessed: 28 April 2011.

2. "Digital Potentiometer". URL `http://www.analog.com/static/imported-files/data-sheets/AD5220.pdf`. Accessed: 28 April 2011.

3. "Frequency Mixer". URL `http://www.minicircuits.com/pdfs/SYM-30DLHW.pdf`. Accessed: 28 April 2011.

4. "Rice University WARP Project". URL `http://warp.rice.edu`. Accessed: 5 January 2012.

5. "Spectrum Analysis Basics". URL `http://cp.literature.agilent.com/litweb/pdf/5952-0292.pdf`. Accessed: 18 May 2011.

6. "Sun Spot World". URL `http://www.sunspotworld.com/vision.html`. Accessed: 18 May 2011.

7. "Voltage Controlled Oscillator". URL `http://www.minicircuits.com/pdfs/JTOS-3000.pdf`. Accessed: 28 April 2011.

8. "Report on Wireless Location-Based Markets". PELOUS Group, NJ, Tech. Rep., 2001.

9. "Wi-Fi Location-Based Services (4.1 Desing Guidie)", May 2008. URL `http://www.cisco.com/en/US/docs`. Accessed: 18 July 2011.

10. Anderson, Chris. "Poor Man's Spectrum Analyzer", August 2010. Version 1.

11. Bertinato, M., G. Ortolan, F. Maran, R. Marcon, A. Marcassa, F. Zanella, P. Zambotto, L. Schenato, and A. Cenedese. "RF Localization and Tracking of Mobile Nodes in Wireless Sensor Networks: Architectures, Algorithms and Experiments". URL `http://paduaresearch.cab.unipd.it/1046/1/EWSN08`.

12. Chen, Y. and H. Kobayshi. "Signal Strength Based Indoor Geolocation". *IEEE Int. Conf. Communications*. May 2002.

13. Defense Acquisition University. *Defense Acquisition Guidebook*, January 2012.

14. Dogandzic, A., J. Riba, G. Seco, and A. Lee Swindlehurst. "Positioning and Navigation with Applications to Communication". *IEEE Signal Processing Mag*, vol. 22, no. 4:10–11, July 2005.

15. Franklin, C. and J. Laxton. "How Bluetooth Works [Online]". URL `http://electronics.howstuffworks.com/bluetooth2.htm`. Accessed: 14 July 2011.

16. Hardy, T.J. *Malicious and Malfunctioning Node Detection via Observed Physical Layer Data*. Master's thesis, Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, March 2011.

17. Kay, Steven M. *Fundamentals of Statistical Signal Processing Estimation Theory*. 18th Printing. Prentice Hall PTR, Upper Saddle River, New Jersey 07458, 2010.

18. King, Amanda. "Development of a Model and Localizaiton Algorithm for Received Signal Strength Based Geolocation", November 2011. Air Force Institute of Technology, PhD Prospectus.

19. Krizman, K. J., T. E. Biedka, and T. S. Rappaport. "IEEE 47th Vehicular Technology Conference". *Wireless Position Location: Fundamentals, Implementation Strategies, and Sources of Error*. May 1997.

20. Lehmann, E. and G. Casella. *Theory of Point Estimation*. New York: Springer, 1998.

21. Martin, R. K. "Emitter Geolocation via Signal Strength, EENG 663 Class Project, Spring 2011", 2011.

22. Martin, R. K., A. S. King, R. W. Ryan, and J. R. Pennington. "Practical Limits in RSS-Based Positioning". *IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP)*. May 2011.

23. Pages-Zamora, A., J. Vidal, and D. H. Brooks. "Closed-Form Solution for Positioning Based on Angle of Arrival Measurements". *The 13th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*. September 2002.

24. Palhlavan, K., X. Li, and J. Makela. "Indoor Geolocation Science and Technology". *IEEE Communications Magazine*, 40, no. 2:112–118, February 2002.

25. Patwari, N., J.N. Ash, S. Kyperountas, A.O. Hero III, R.L. Moses, and N.S. Correal. "Locating the Nodes. Cooperative Localization in Wireless Sensor Networks". *IEEE Signal Processing Magazine*, 22, no. 4:10–11, July 2005.

26. Rappaport, T.S., J. H. Reed, and B. D. Woerner. "Position Location Using Wireless Communications on Highways of the Future". *IEEE Communications Magazine*, 34, no. 10:33–41, October 1996.

27. Sayed, A., A. Tarighat, and N. Khajehnouri. "Network-Based Wireless Location: Challenges Faced in Developing Techniques for Accurate Wireless Location Information". *IEEE Signal Processing Magazine*, 22, no. 4:24–40, July 2005.

28. Sun, G., J. Chen, W. Guo, and K. Liu. "Signal Processing Techniques in Network-Aided Positioning". *IEEE Signal Processing Magazine*, 22, no. 4:12–23, July 2005.

29. Sun Labs. *Sun SPOT Theory of Operation, Red Release 5.0*, July 2009.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704–0188

1. REPORT DATE *(DD–MM–YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From — To)*
22–03–2012	Master's Thesis	Sept 2010 — Mar 2012

4. TITLE AND SUBTITLE

Low Cost, Low Complexity Sensor Design for Non-Cooperative Geolocation via Received Signal Strength

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Butler Michael S., Captain, USAF

5d. PROJECT NUMBER

ENG09-182

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GE/ENG/12-05

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Vasu Chakravarthy
Air Force Research Laboratory, Sensors Directorate, Electronic Warfare Branch
2241 Avionics Circle, Bldg 620
Wright-Patterson AFB, OH, 45433-7301
DSN: 785-5579 x4245
vasu.chakravarthy@wpafb.af.mil

10. SPONSOR/MONITOR'S ACRONYM(S)

AFRL/RYWE

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Obtaining accurate non-cooperative geolocation is vital for persistent surveillance of a hostile emitter. Current research for developing a small, cheap and energy efficient sensor network for non-cooperative geolocation measurements via received signal strength (RSS) is limited. Most existing work focuses on simulating a non-cooperative network (NN) and in doing so, simulated models often ignore localization errors caused from the hardware processing raw RSS data and often model environment-dependent errors as random. By comparing real-time measured non-cooperative geolocation data to a simulated system a more accurate model can be developed. This thesis discusses the development and performance of a small, low cost, low complexity, and energy efficient sensor network that can locate a NN via RSS. The main focus of this research effort is designing a Poor Man's Spectrum Analyzer (PMSA) to locate a wireless device in a non-cooperative network (NN) that is transmitting in the Industrial, Scientific and Medical (ISM) radio band of 2.403 GHz to 2.48 GHz by measuring the emitter's received signal strength (RSS).

15. SUBJECT TERMS

Non-Cooperative Geolocation, Received Signal Strength, Maximum Likelihood Estimation, Poor Man's Spectrum Analyzer

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Richard K. Martin, PhD (ENG)
U	U	U	UU	89	19b. TELEPHONE NUMBER *(include area code)* (937) 255–3636, x4625; Richard.martin afit.edu